



פרסומי מרכז דדו

06/2017

הרתעה בסב"ר - תיאוריה ואתגרים

סקירת התפתחות הגישות בספרות המקצועית

המערבית

שמואל שמואל

בלמ"ס

תמוז תשע"ז – יולי 2017

פתח דבר

מרחב הסב"ר הוא מרחב חדש וייחודי. ככזה, הפעולה האנושית בו מביאה עימה מגוון סוגיות חדשות עבור מערכת הביטחון. אופיו הייחודי של המרחב – חשאיותו, "עכירותו" ואף חדשנותו – מביא לכך שתופעות מוכרות מקבלות בו פנים חדשות.

דוגמא לתופעה שכזו היא ההרתעה. סוגיית ההרתעה היא מן המורכבות הקיימות בשדה היחסים הבין לאומיים ומרחב הסב"ר מוסיף על מורכבות זו הן עקב טבעו והן עקב החידוש בו. תקפות חלק ממרכיבי ההרתעה הבסיסיים ביותר – האיתות ליריב, הפגנת היכולות והתוצא ברור והניתן לחזוי מראש – אינה ברורה במרחב הסב"ר, ובכך מעמידה בסימן שאלה את הרלוונטיות של מונח זה.

בעת זאת, כאשר הולכות ומתהוות התפיסות הבסיסיות למרחב הסייבר, קיימת הזדמנות ייחודית למצוא פתרונות מקיפים ויסודיים למגוון סוגיות הקשורות בפעולה במרחב הסב"ר ולאופן הפעולה הצבאית במרחב זה.

מחקר זה נועד להאיר מספר היבטים של ההרתעה בסב"ר על מנת ליצר תשתית מקצועית ראשונית לדיון בנושא. המחקר כולל סקירה מעובדת של מקורות מערביים עדכניים הדנים בסוגיה.

המחקר נועד לסייע לחשיבה המתרחשת כעת בנוגע לתפיסת ההפעלה הצבאית במרחב הסב"ר, באמצעות התמקדות בסוגיית ההרתעה. מטרת המחקר היא בעיקר להעלות סוגיות לדיון והוא אינו עוסק במציאת פתרונות לסוגיות אלה.

המחקר נכתב במסגרת פרויקט פיתוח ידע לתחום הסב"ר במרכז דדו.

המחקרים הקודמים בסדרה זו הם:

- סוגיות אזרחיות הנוגעות לפעולת המדינה במרחב הסב"ר.
- מערך המילואים בסב"ר של ארה"ב, בריטניה ואסטוניה.
- כוחות בלתי סדירים בסב"ר.

המחקר נכתב ע"י מר שמואל שמואל, חוקר סב"ר וצבאות זרים במרכז דדו.

בלמ"ס

קריאה פורייה,

תא"ל (מיל") מאיר פינקל

מפקד מרכז דדו

תוכן העניינים

7	מבוא
9	פרק א' – רקע תיאורטי לנושא ההרתעה
15	פרק ב' – גישות המקובלות כיום בנוגע להרתעה במרחב הסב"ר
17	פרק ג' – אתגרי ההרתעה בסב"ר
25	פרק ד' – מימוש ההרתעה בסב"ר
35	סיכום ומסקנות
41	נספח א' – קיצור תולדות ההרתעה (בעת המודרנית)
48	רשימת מקורות

מבוא

"אף אחד לא אחד העז לקרוא תיגר על האויב ואף לא אחד היה מוכן לפגוע בו כאשר ידע שהוא נמצא בעמדה טובה יותר ומוכן להילחם".

פלביוס ווגטיוס רנטוס, **העיסוק הצבאי (De Rei Militari)**, ספר שלישי¹

¹ פלביוס ווגטיוס רנטוס, "העיסוק הצבאי", בתוך: אמ"ץ-תוה"ד, **אודות העיסוק הצבאי**, תצפית 72, 2012, ע' 120.

בהתנהלותן הבינ"ל, מנסות מדינות רבות להימנע ככל האפשר מכניסה לעימותים חמושים. באופן מסורתי, נחשב העימות החמוש ל"טיעון האחרון של המלכים"² ולהמשך הפוליטיקה באמצעים אחרים. חלק מרכזי מהניסיון לדחות את העימות נעשה לעתים רבות באמצעות מאמץ לשכנוע הצד השני שהעימות אינו כדאי לו – או במילה אחרת, הרתעה.

רעיון ההרתעה הוא רעיון עתיק. את התפיסה לפיה "הרוצה בשלום, יכון למלחמה" אפשר למצוא עוד בכתיבה מהתקופה הרומאית. עם זאת, כשהם שהיא עתיקה, כך ההרתעה קשה להגדרה וליישום. עם הופעת הנשק הגרעיני, הפך הצורך להימנע ממלחמה לקיומי גלובלי ובהתאם, הפכה ההרתעה לתפיסת מפתח ביחסים הבין לאומיים, הדיון בנושא פרח, נוספו הגדרות והמשגות, והנושא הפך למורכב וקשה להבנה עבור מי שאינו בקיא ברזי התיאוריה היחב"לית.

מטבע הדברים, מנסות מדינות ליישם את ההרתעה בכל המרחבים בהם הן פועלות. הופעת הסביבה הרשתית (סב"ר – Cyber), הביא מדינות שונות וגופים לבחון האם אפשר ליישם את תפיסת ההרתעה גם שם, וכיצד אפשר לעשות זאת.

בהתאם, הכתיבה התיאורטית בנושא רבה, גם בהתחשב בחידוש היחסי שבמרחב הסב"ר. עם זאת, המורכבות המובנית שבמרחב הסב"ר וחוסר הבהירות בנוגע להתנהלות בו באופן כללי מקשים מאוד על יישום ההרתעה בו. לפיכך, אין הסכמה במחקר בנוגע לאופן יישום ההרתעה בסב"ר ואף בנוגע לעצם היכולת להגיע אליה.

עבודה זו תנסה לבחון את סוגיית ההרתעה במרחב הסב"ר על בסיס חלק נבחר מהכתיבה שנערכה על הנושא עד כה. היא תבחן את מושג ההרתעה באופן כללי, מקצת מהאתגרים העומדים בפני ההרתעה במרחב הסב"ר ומספר מענים לאתגרים אלה. עבודה זו תהיה תיאורטית בעיקרה ותנסה להביא את הדעות הקיימות בנכר.

מחקר זה יהיה מחולק למספר חלקים כדלהלן: ראשית, תוצג סקירה תיאורטית קצרה על מושג ההרתעה באופן כללי. העבודה אינה נועדה לדון במושג ההרתעה לכשעצמו. לכן, יסתמך רוב החלק התיאורטי על ספרו המקיף של לורנס פרידמן בנושא, שמכיל את תמצית ההגות העדכנית (יחסית) בתחום. לאחר מכן, יסקרו מספר אתגרים ליישום ההרתעה ומספר מענים אפשריים לאתגרים אלה. כיוון שתחום הסב"ר הוא תחום מתהווה, המשתנה תדיר, ניסה המחקר לבחון מקורות עדכניים בלבד וכמעט לא בחן כתיבה מלפני שנת 2011. אומנם היו מספר מחקרים משמעותיים שנכתבו בנושא גם לפני כן, אך הכתיבה העדכנית יותר מכילה בתוכה גם את התובנות של המחקרים המשמעותיים המוקדמים. כיוון שתפיסת ההרתעה הגרעינית מקרינה באופן משמעותי על הנכתב בעולם על ההרתעה באופן כללי, תובא בנספח א' סקירה קצרה של ההרתעה בעת המודרנית ושל ההרתעה הגרעינית באופן שנתפסה

² Ultima ratio regum - ביטוי אותו חקק המלך לואי ה-14 על תותחיו.

במערב ובברה"מ. כך, ינסה המחקר לבחון באופן כללי מה הם מאפייני ההרתעה בסב"ר והאם יש נושאים עליהם קיימות הסכמות משמעותיות בקרב העוסקים בנושא – ולכן אפשר לראות בהם כסוג של "עוגנים תיאורתיים" מתהווים, מהם אפשר להתחיל את הדיון הרחב יותר. יש לציין, עם זאת, שהמחקר כולל בעיקר חומרים מערביים. לשם השלמת התמונה, יש לבחון באופן מעמיק יותר כיצד תופסים גורמים אחרים – בעיקר גורמים במזה"ת, הרוסים והסינים – את ההרתעה בסב"ר. אם בחינת ההרתעה במלחמה הקרה עשויה ללמד אותנו דבר מה, הרי שמדובר בפערים התפיסתיים האפשריים בכל הנוגע להרתעה, אפילו זו הגרעינית, בין שחקנים שונים.

פרק א' – רקע תיאורטי לנושא ההרתעה

ברמה הבסיסית ביותר, ההרתעה היא הצבת גבולות לפעולות מסוימות ויצירת סיכונים הכרוכים בחציית גבולות אלה. נהוג להגדיר הרתעה כאסטרטגיה כפייתית, המסתמכת על ניסיונות מכוונים לשנות את ההתנהגות של האחר (ובייחוד – להביאו להימנע מביצוע מעשים מסוימים) באמצעות איומים מותנים וגלויים (כנים או כוזבים) לשימוש בכוח. הרתעה היא מערכת יחסים וככזו, היא אינה עומדת בפני עצמה, אלא היא חלק ממגוון נרחב של מערכות יחסים³ - איומים מותנים הם אמצעי תקשורת ככל האחרים ועליהם להתלוות לצורות תקשורת אחרות.⁴

אפשר להנגיד את ההרתעה לכפייה/אכיפה (Compellence/Coercion)⁵. הרתעה פירושה לגרום לפלוני לא לעשות דבר מה שהוא רוצה לעשות. כפייה/אכיפה היא לגרום לפלוני לעשות דבר מה שהוא אינו מעוניין לעשות. בהתאם, ההרתעה בדרך כלל מכוונת לשמור על הסטטוס קוו ואילו הכפייה/אכיפה מכוונת לשנותו. עם זאת, אפשר ששתי הגישות נמצאות על רצף אחד ושההבדלים בניהן נעלמים לאחר שעומות הסלים- אז יעשה שימוש בו זמני הן בהרתעה והן בכפייה/אכיפה.⁶

הגישה התועלתנית (Utilitarian)⁷ טוענת שכדי שההרתעה תהיה יעילה, נדרשות מידת בהירות של העונש הצפוי, יכולת חיזוי שלו על ידי המורתע ומידתיות בין העבירה לבין העונש. לתפיסה זו, המקובלת בעיקר בתחומי הדין הפלילי וענישת פושעים, יש מגבלות בזירה הבין לאומית כיוון שאין בה סמכות ריבונית המסוגלת לכפות חוקים ולהחזיק במונפול על הפעלת האלימות ואילו לגורמים שונים במערכת יש יכולת להגיב לעונש שיושג עליהם.⁸ עם זאת, היא מסבירה את שלוש הרגליים הבסיסיות של ההרתעה – בהירות המסר, אמינות ההרתעה ומידתיות העונש.

כדי שתהיה אמינה, מצריכה ההרתעה שני מרכיבים – הכוונה המוצהרת של המרתיע להגן על אינטרס מסוים והיכולת להגן על אינטרס זה – או לחילופין, תפיסה של המורתע לפיה ההפרה של האינטרס של המרתיע תעלה לו ביוקר. או במילים אחרות, כוונה ויכולת. לכל הרתעה נדרש מסר מרתיע שיועבר ליריב. המסר המרתיע והעברתו (Signaling) אמורים לכלול הן את האינטרס שיש להגן עליו והן את האיום שיופעל במקרה שהאינטרס יופר. מסר זה

³ המצב במלחמה הקרה היה, לפיכך, יוצא דופן.

⁴ Lawrence Freedman, *Deterrence*, Cambridge, UK: Polity Press, 2004, pp. 3, 6, 26-27. 116

⁵ או בצה"ל – אכיפה. למחקר בענייני אכיפה בצה"ל ראה:

יניב פרידמן, אכיפה – הגיון פעולה נוסף לאסטרטגיית צה"ל, פרסומי מרכז דדו 02/2017, פברואר 2017

⁶ Lawrence Freedman, *Op. cit.*, pp. 110-111

⁷ בהקשר של ענישת פושעים.

⁸ *Ibid*, pp. 8-9

צריך להיות ברור, אך לרוב לא נאמר באופן ישיר וברור.⁹ כיוון שמדיניות הרתעתית עשויה לערער יציבות, המרתיע חייב להיות מסוגל להסביר אותה לדעת הקהל הפנימית והבין לאומית שלו, כדי להצדיק את המדיניות בזמן שגרה ואת ההסלמה במקרה הצורך. כמו כן, יש צורך להבהיר ליריב שהמדיניות היא הרתעתית באופייה ולא תשמש למתקפה מקדימה – דבר המחייב הכרה טובה של היריב.¹⁰

ההרתעה היא גישה המצריכה איזון – הרתעה חלשה מידי לא תהיה יעילה ואילו הרתעה חזקה מידי עשויה להתפרש כתוקפנות וכך להיכשל. כך, לדוגמה, הפכה ההרתעה הגרעינית למדיניות שהצריכה הפחדה של המעצמה השנייה כדי למנוע ממנה לעשות מעשים מסוימים מחד גיסא ומאידך גיסא הרגעה של אותה המעצמה כדי למנוע ממנה להיות תוקפנית מידי.¹¹ היעדר איזון עשוי להוביל לתהליך הסלמה בלתי נשלט בו שני צדדים עלולים להגיע לעימות (אפילו גרעיני) ללא כוונה, כתוצאה מתהליך הסלמה הדרגתי ואינטראקטיבי (הדדי), בו כל צד מקבל, באופן רציונלי, החלטות מסלימות כתגובה על החלטות הצד השני.¹² ההרתעה היא נושא שנכתב עליו רבות במהלך המלחמה הקרה. כתיבה זו הביאה לפיתוחם של מספר מושגים בסיסיים בתחום:

מקור ההרתעה: בתחום זה יש שתי הגדרות הנוגעות למהות ההרתעה – האם היא נובעת מאיום גלוי וברור, או שמא מהבנה של המורתע שאינה בהכרח נובעת מאיום גלוי.

- הרתעה אסטרטגית (Strategic Deterrence): אפשרות אסטרטגית הזמינה לשחקן א' (החושש לפגיעה באינטרסים שלו משחקן ב') המתבטאת בהתחייבות מפורשת לנקוט צעדים "משמעותיים"¹³ נגד שחקן ב', אם שחקן ב' יפעל באופן מסוים נגד רצונותיו של שחקן א'. כדי להשיג הרתעה אסטרטגית, שחקן ב' צריך להאמין שכל צעד תוקפני שלו נגד שחקן א' יכשל – בין אם עקב התנגדותו של שחקן א' ובין אם עקב תגובתו, שתפגע בשחקן ב' עד כדי כך שהנזק יעלה על הרווח הצפוי. ההרתעה האסטרטגית מתבססת על ההנחה שהשחקנים רציונליים, שהאיומים נהירים לשני הצדדים ואמינים וששחקן א' יכול לחזות מה תהיה תגובתו של שחקן ב' לאיומו. בעוד שקל להוכיח שהרתעה אסטרטגית נכשלה, קשה יותר להוכיח האם היא עובדת.¹⁴

⁹ Annegret Bendiek, Tobias Metzger, *Deterrence Theory in the Cyber-Century*, Working Paper RD EU/Europe 2015/02, Berlin: German Institute for International and Security Affairs, May 2015, p. 5

¹⁰ Jonathan F. Solomon, "Demystifying Conventional Deterrence – Great Power Conflict and East Asian Peace", *Strategic Studies Quarterly*, Winter 2013, p. 127

¹¹ Lawrence Freedman, *Op. cit.*, p. 15-16

¹² Jonathan F. Solomon, *Op. cit.*, p. 131

¹³ הן צעדי ריסון והן צעדי ענישה.

¹⁴ Lawrence Freedman, *Op. cit.*, pp. 27-29

● הרתעה מופנמת (Internalized Deterrence): הרתעה שאינה מגיעה כתוצאה מאיום גלוי ומודע. כלומר, שחקן ב' מורתע לעשות דבר מה הפוגע בשחקן א', לא מפני ששחקן א' איים עליו בגלוי, אלא מכיוון ששחקן ב' מאמין שהעלויות של פעולתו תהינה גדולות מהרווח שינבע מהן. חישוביו של שחקן ב' עשויים להיות מבוססים או מופרכים ועשויים להיות ידועים לשחקן א' או לא. הרתעה זו נפוצה הרבה יותר מההרתעה האסטרטגית. הרתעה מופנמת עשויה לנבוע מאיום שעם הזמן הופנם על ידי המורתע ולכן אין המרתיע צריך להשתמש בו עוד באופן פעיל. למעשה, לרוב, אתגר המדיניות המשמעותי הוא להפוך הרתעה אסטרטגית להרתעה מופנמת.¹⁵

אמינות (Credibility): המידה בה האויב מאמין שהמדינה המאיימת תממש את האיום. האמינות קשורה בשאלה האם הנושא שבהקשרו הוצג האיום שווה את המאמץ (והעלות) של יישום האיום. דרך אחת להעריך את מידת האמינות של איום מסוים היא על פי עמידה באיומים ובהתחייבויות קודמות. כך, כל התחייבות, קטנה ככל שתהיה, עשויה להפוך לעקרונית כיוון שהיא משליכה על אמינות האיומים וההתחייבויות בעתיד.

סוגי הרתעה: ההרתעה אינה דבר אחיד, אלא מתחלקת לכמה סוגים. את ההרתעה אפשר לסווג לפי מנעד המעשים אותם היא מנסה להרתיע, הכלים אותם היא מפעילה והנסיבות בהן היא שוררת.¹⁶

● מנעד ההרתעה:

○ הרתעה צרה/ממוקדת (Narrow): הרתעה כנגד מבצעים מסוג מסוים במהלך מלחמה (הפצצות אסטרטגיות, שימוש בנשק להשמדה המונית וכו).¹⁷

○ הרתעה רחבה/בסיסית (Broad): הרתעה מפני פתיחה של מלחמה כל שהיא, באופן כללי.

● נושא ההרתעה:

○ הרתעה מורחבת (Extended): הרתעה מפני תקיפה של בעל ברית או גורם שלישי כל שהוא.

○ הרתעה מרכזית (Central): הרתעה של גורם מפני תקיפתו על ידי גורם אחר.

● אסטרטגיית ההרתעה:

¹⁵ Ibid, pp. 29-32

¹⁶ Ibid, pp. 32-42

¹⁷ יש הטוענים שהנשק הכימי והיעדר שימוש באירופה במלה"ע 2 מספק דוגמה להרתעה משימוש באמל"ח תוך כדי עימות. הרתעה זו מקורה הן בפחד מתגובה והן במידת השימושיות המוגבלת של האמל"ח.

Ibid, p. 71

○ הרתעה באמצעות מניעה (Denial): הרתעה באמצעות מניעת רווח מהתוקף. זאת על ידי יצירת שליטה במצב במידה מספיקה, כדי למנוע מהאויב אפשרויות פעולה "זולות" או רווח מספיק מהן. על ידי כך, השאיפה היא ליצור מצב בו יהיה על התוקף לשאת בעלויות ניכרות אם ברצונו לממש רווח מאפשרות פעולה מסוימת ושהסיכוי לרווח לכיסוי עלויות אלה יהיה מוטל בספק. נקראת גם הרתעה סבילה¹⁸. אפשר להמשיך אסטרטגיה של הרתעה באמצעות מניעה להצבת שומרים, מצלמות וסורגים בבתי עסק. המטרה של אמצעים אלה היא להפוך את הפריצה לבית העסק לכה יקרה וקשה ואת סיכויי הכישלון לכה גבוהים, עד שהגנב הפוטנציאלי יבחר לא לעשות זאת, או לחילופין לנסות לפרוץ למקום אחר.¹⁹

○ הרתעה באמצעות ענישה (Punishment): הרתעה באמצעות הגדלת המחיר על פעולת האויב, באמצעות איום בתגמול. נקראת גם הרתעה פעילה.²⁰ אפשר להמשיך אסטרטגיה של הרתעה באמצעות ענישה למערכת השיטור והדין הפלילי. המטרה של מערכות אלה הן למצוא את הפושע, לזהותו בוודאות, להעמידו לדין ולהעניש אותו על מעשיו – עונש שיהיה מספיק כדי למנוע ממנו לעשות את המעשה הפלילי. ההרתעה הזו אמורה לפעול לא רק על הפושע עצמו, אלא על הסובבים אותו. כדי שהיא תתפקד, סיכויי האיתור וההרשעה חייבים להיות גבוהים יחסית, בנוסף לכך שהעונש חייב להיות חמור דיו (אך לא חמור מידי) כדי להרתיע.²¹

○ הרתעה מותאמת (Tailored Deterrence): הרתעה המושגת באמצעות שילוב בין הגדלת העלויות עבור היריב (באמצעים השונים מאיום בהתקפה) ובין מניעת הישגים מהיריב (כולל באמצעות צמצום ההשלכות השליליות מתקיפה אפשרית).²²

● נסיבות ההרתעה:

○ הרתעה מיידי (Immediate): הרתעה במהלך משבר. מערכת היחסים בין שחקנים, כאשר לפחות אחד מהם שוקל ברצינות לפתוח בהתקפה בעוד שאחרים מאיימים להגיב כדי למנוע את ההתקפה.

○ הרתעה כללית (General): הרתעה המתרחשת כאשר שחקנים חמושים מווסתים את מערכת היחסים בניהם בלי שאחד מהם שוקל לפתוח בהתקפה מיידי. ההרתעה הכללית פועלת במהלך ימי השגרה באמצעות הבהרה ליריב שאין טעם לפעול

¹⁸ Clorinda Trujillo, "The Limits of Cyberspace Deterrence", *JFQ* 75, 4th Quarter, 2014, p. 45

¹⁹ Lawrence Freedman, *Op. cit.*, p. 60

²⁰ Clorinda Trujillo, *Op. cit.*, p. 45

²¹ Lawrence Freedman, *Op. cit.*, p. 60

מובן שבמערכת הפלילית לענישה יש גם תפקיד של גמול כלפי העבריין ולא רק תפקיד הרתעה, אך זה אינו הדין כאן.

²² Franklin D. Kramer and Aelanie J. Teplinsky, *Cybersecurity and Tailored Deterrence*, Atlantic Council, Dec. 2013, p. 2

באמצעים אלימים וזאת גם ללא הפגנות כוח פעילות ורציפות על ידי המרתיע. ההרתעה הכללית מצריכה שהמורתע יפנים את האיום של המרתיע ויאמין שהאיום אמין וסביר.

● אמצעי ההרתעה:

○ הרתעה על בסיס ערכים: הרתעה המבוססת על ערכים הנתפסים ככאלה שאין להפר. בזירה הבינ"ל אפשר לראות זאת בניסיון למנוע מעשים שנחשבים כ"טאבו", כגון שימוש בנשק גרעיני (או במיקוש או בנשק מצרר).²³ עם זאת, יש לזכור שיש יחסית מעט מעשים בזירה הבינ"ל הנחשבים כטאבו ואפשר שאין אף מעשה יחיד הנחשב כטאבו אוניברסלי.

○ הרתעה על בסיס אינטרסים: הרתעה באמצעות איום על אינטרסים של השחקן השני.
○ הרתעה על ידי הרגעה (Reassurance): יישום הרתעה באמצעות וויתור מוכרז על יכולות או על קווי מדיניות מסוימים, כדי למנוע מהיריב לנקוט במעשים מערערי יציבות, בתגובה על פעולות שהוא חושב שהצד המרתיע ינסה לעשות נגדו. בזירה הגרעינית הרתעה באמצעות הרגעה יושמה על ידי הכרזה על הימנעות משימוש ראשון בנשק גרעיני (No First Use Policy) ועל ידי פירוק יכולות שילוח מסוימות כגון טילים בליסטיים וטילי שיוט לטווחים בינוניים ולטווחי ביניים.²⁴

יש הטוענים שאפשר לפרק את ההרתעה לשמונה מרכיבים:²⁵

- אינטרס (האינטרס שמבקשים להרתיע מפני התקפתו);
- הכרזה מרתיעה (אם יעשה X, התגובה תהיה Y);
- אמצעי מניעה (צמצום התועלת הנובעת משבירת ההרתעה);
- אמצעי ענישה (ענישה על שבירת ההרתעה);
- אמינות (מידת האמינות של ההכרזה המרתיעה);
- הרגעה (אם ההרתעה לא תישבר, לא יאונה למורתע כל רע);
- פחד;
- תחשיב עלות-תועלת של היריב בנוגע לשבירת ההרתעה;

הרתעה מתבססת בהכרח על יכולות ברורות ואמינות ליישם את האיום. אמינות ההרתעה נקבעת על פי שילוב של היכולות הקיימות, הכוונה להשתמש ביכולות אלה וחוסר היכולת לערער הן על היכולות והן על הכוונה להשתמש בהן (כפועל יוצא מוודאות קיומה של היכולת,

²³ Lawrence Freedman, *Op. cit.*, p. 70

²⁴ Will Goodman, "Cyber Deterrence – Tougher in Theory than in Practice?", *Strategic Studies Quarterly*, Fall 2010, p. 107

²⁵ *Ibid.*, p. 105

מחומריתה וממידיות הפעלתה – הן כתוצאה מתקדימים היסטוריים והן כתוצאה מהכרזת כוונות ומדיניות נוכחית).²⁶ עם זאת, הצלחת אסטרטגיה של הרתעה אינה מובטחת כיוון שהיא מבוססת על שיתוף פעולה של כל הצדדי הנתונים בעימות ולכן היא תמיד תהיה נתונה לספק.²⁷ בהינתן הנשק הגרעיני והסכנה העולה ממנו, עיקר העיסוק בהרתעה במהלך שנות המלחמה הקרה (וגם לאחר מכן) נגע בסוגיה הגרעינית ולא היה עיסוק ניכר בתיאוריה של הרתעה מוסכמית (קונבנציונלית). יש שטענו שהרתעה מוסכמית טמונה ביכולת לשכנע את היריב שמתקפה צבאית שיערוך לא תצליח להשיג את יעדיה. בהקשר זה (ומתוך הדוגמה הישראלית), יש שטענו שאפשר לפתח הרתעה מתוך מוניטין הנוצר מהפעלה חוזרת ונשנית של כוח. הרתעה שכזו תדרוש "תחזוקה שוטפת" כדי לקיימה. כך, ההרתעה הקונבנציונלית מצריכה הדגמת יכולות – ובכך יש שוני מהותי מההרתעה הגרעינית (שמטבע הדברים, אינה יכולה לאפשר "הדגמה" של יכולות²⁸). הדגמת יכולות זו עשויה שלא להתאפשר פוליטית כאשר היא נדרשת "הרתעתית" וכמו כן לעמוד במתח עם הצורך "לשמור על הסוד" כדי למנוע מהיריב ללמוד לסתור את העוצמה הצבאית של המרתיע.²⁹ בשונה מהרתעה גרעינית, הרתעה מוסכמית אינה "הרמטית". לכן היא יכולה להתבסס יותר על "מניעה" ופחות על ענישה. כך, לא נדרש שכנוע היריב בכך שכל פעולה צבאית שלו תובס ללא קושי, אלא די בכך שהיריב יאמין שלמרתיע די כוחות צבאיים, ברמה טובה מספיק, במוכנות גבוהה מספיק וקרבה רבה מספיק, כדי שיהיה סיכוי ניכר שכל התקפה שיערוך היריב על המרתיע תידרדר לכדי עימות ארוך, מסוכן, יקר ובלתי מוכרע. ליבת ההרתעה המוסכמית על ידי מניעה נובעת מעמידות המרתיע להתקפת פתיחה, כך שהוא יוכל לעמוד בה ולגרום נזק מספיק לאויב כדי למנוע ממנו מלהשיג את מטרותיו.³⁰

הרתעה מוסכמית מתבססת על הנחה שהיריב משתמש בסולם ערכים מסוים, המבוסס על חישובי סיכון-תועלת "רציונאליים" של העולם הזה בלבד. גם במקרה זה, ההרתעה עשויה שלא לעבוד במקרה שהיריב סבור שמאזן הכוחות הצבאי הולך ונוטה לרעתו באופן בלתי הפיך, עד כדי כך שבעתיד כוחותיו לא יספיקו כדי לערוך פעולה צבאית כלשהי. הרתעה כזו עשויה גם שלא לעבוד גם אם היריב חשוף ללחצים פנימיים, אם הוא מעריך לא נכון את מאזן הכוחות, מגזים בהערכת יכולותיו שלו, ממעיט בהערכת האינטרסים של המרתיע, מידת מחויבויותיו ונכונותו להילחם או אם הוא סבור שהמרתיע מנצל את הזמן להתעצמות ואין ספק שיתקוף

²⁶ Will Goodman, *Op. cit.*, p. 106

²⁷ Lawrence Freedman, *Op. cit.*, pp. 117-118

²⁸ אומנם ישנם ניסויים גרעיניים המאפשרים הדגמה מסוימת של יכולות גרעיניות. עם זאת, כל הניסויים הללו (ואף ההרתעה הגרעינית בכלל) נשענים במידה רבה על השימוש המבצעי היחיד שנעשה, עד כה, בנשק גרעיני בסוף מלה"ע השנייה.

²⁹ Lawrence Freedman, *Op. cit.*, p. 38-39

³⁰ Jonathan F. Solomon, *Op. cit.*, p. 118-119

אותו בעתיד. מנגד, הרתעה מוסכמית מבוססת על ענישה באמצעות איום בהפעלת כוח עשויה להיכשל, במיוחד כנגד יריבים בעלי סף סבילות גבוה לסיכונים או כנגד יריבים המונעים מפחד או מייאוש.³¹

הדיון הנרחב בהרתעה התקשה מאוד לבחון באופן אמפירי האם ההרתעה עובדת באופן כללי ואיזה סוג של הרתעה עובד באופן ספציפי. זאת מכיוון שקשה מאוד לקבוע מה הם המשתנים התלויים, מה הם המשתנים הבלתי תלויים ומה הם היחסים בניהם, בעולם שבו ההחלטות של הצדדים השונים מושפעות הדדית אחת מהשנייה ומגורמים רבים נוספים. כמו כן, קשה מאוד למצוא מספר רב מספיק של מקרי מבחן דומים מספיק לשם בחינת תיאוריות שונות של הרתעה. לבסוף, קשה מאוד להוכיח שההרתעה הצליחה, כיוון שהדבר כרוך בהוכחת דבר מה שלא קרה³² - "המורתע" אומנם לא עשה מעשה מסוים אך, לא תמיד ברור האם הוא התכוון לעשותו מלכתחילה ולמה הוא לא עשה זאת בסופו של דבר. עם זאת, יש הבנה במחקר שאיומים של המרתיע עשויים שלא להשפיע על הצד המורתע כלל, או לחילופין שהצד המורתע עשוי להיות מורתע או מושפע מסיבות שונות, שאינן קשורות (ישירות או בעקיפין) לאיומי המרתיע. זאת בלי להזכיר את מגוון הקהלים והאינטרסים המושפעים מניסיונות ההרתעה או שאותם באים ניסיונות אלה לשרת.³³ לפיכך, כל סוגיית ההרתעה נחשבת ביחב"ל לבעייתית מלכתחילה ולקשה להבנה ותכנון.

עקב כך, ההרתעה נחשבת לעניין גמיש ואף "אמורפי". סוגי הרתעה שונים משלימים זה את זה. לדוגמה, הרתעה גרעינית הדדית והרתעה מוסכמית על ידי עוצמה צבאית מוסכמית איתנה משלימות אחת את השנייה. כך, הן מונעות הן הפעלת נשק גרעיני (הן אסטרטגי והן טקטי) והן ניסיון להשיג יעדים על ידי פעולה מוסכמית מוגבלת (או איום בפעולה כזו) שתישאר מתחת לסף הגרעיני.³⁴ לפיכך, לא כל הרתעה תכלול גם אמצעי ענישה וגם אמצעי מניעה ולעומת זאת, במקרים מסוימים תכלול ההרתעה גם אמצעים כאלה וגם אמצעים כאלה.³⁵ כמו כן, יש לזכור שההרתעה חשופה תמיד גם למאמצי הלמידה של היריב. לפיכך, היא מחייבת מאמץ הסתגלות מתמיד, הכולל הערכת מצב מתמדת, בשילוב משחקי מלחמה וניסויים שונים, המשקללים את כלל מרכיבי ההרתעה אל מול היריב, הסביבה וההקשר ומתאימים את הכוח, השיטות והתפיסות למציאות החדשה.³⁶

³¹ *Ibid*, p. 119-120

³² הדבר נכון במיוחד כאשר באים לבחון הרתעה כללית, על פני משך זמן ארוך.

³³ Lawrence Freedman, *Op. cit.*, pp. 44-45, 58-59

³⁴ Jonathan F. Solomon, *Op. cit.*, p. 135

³⁵ Will Goodman, *Op. cit.*, p. 106

³⁶ Jonathan F. Solomon, *Op. cit.*, pp. 147-148

בלמ"ס

פרק ב' – גישות המקובלות כיום בנוגע להרתעה במרחב

הסב"ר

קיימות דעות רבות ושונות בנוגע היכולת לקיים הרתעה במרחב הסב"ר באופן כללי ועל דגם ההרתעה הרלוונטי בו בפרט.

ראשית יש לנסות ולהגדיר מה כוללת ההרתעה בסב"ר. אפשר לחלק את המושג להרתעה באמצעות מרחב הסב"ר (Cybered Deterrence) ולהרתעה במרחב הסב"ר (Cyber Deterrence) – כלומר, להרתעה באמצעות פעולות במרחב הסב"ר ולהרתעה מפני פעולות במרחב זה. עם זאת, הקו המפריד בין מרחב הסב"ר למרחבים האחרים מטושטש. פעמים רבות פעולות במרחב הסב"ר משפיעות על מרחבים אחרים ומושפעות מהם ומטרותיהן הן להשפיע על מרחב הסב"ר והן על מרחבים אחרים. לפיכך, קשה להפריד בין פעולות הנעשות באמצעות מרחב הסב"ר לשם השפעה על מרחבים אחרים לבין פעולות הנעשות אך ורק בתוך מרחב הסב"ר ולשם השפעה עליו. כמו כן, כיוון שמהות הפעולות במרחב הסב"ר היא להשפיע על בני אדם, כלל לא ברור אם יש ערך כלשהו בהפרדה שכזו. לפיכך, נראה כי עלינו להכליל את ההרתעה באמצעות מרחב הסב"ר וההרתעה במרחב הסב"ר באותה התפיסה, מתוך טענה שהרתעה במרחב הסב"ר ומחוצה לו מתגברות אחת את השנייה, תלויות אחת בשנייה ואין להפריד ביניהן. לפי תפיסה זו ההרתעה בסב"ר נועדה כדי להניא את האויב מפני פעולות עוינות במרחב הסב"ר ובאמצעותו.³⁷

העיסוק הרב בספרות בהרתעה הגרעינית השפיע על האופן בו רוב צבאות העולם תופסים את נושא ההרתעה באופן כללי, עד היום ומשפיע עקב כך גם על האופן בו הם מנתחים את ההרתעה בסב"ר. כך, מספר רב של מקבלי החלטות – אמריקניים, סינים, רוסים ואחרים – מקבילים בין תקיפות במרחב הסב"ר לתקיפות גרעיניות ומשתמשים בתפיסה הרתעתית באופן כללי, ובפרט בתפיסות ההרתעה הגרעינית, כדי לתת מענה לאתגרי סב"ר שונים - החל מגניבת נתונים של כרטיסי אשראי ועד לפריצות למאגרי מידע מדינתיים. רטוריקה זו, מורשת המלחמה הקרה, נמצאת בשימוש נרחב מאוד בקרב מקבלי ההחלטות האמריקנים ומנסה להשיג הרתעה על ידי איום בתגובה קשה (ואף תגובה מכרעת ובלתי מידתית) וודאית. היא מבטאת ציפייה להרתעה מפני פעילות עוינת במרחב הסב"ר, מוכרת מאוד הן למקבלי ההחלטות והן לציבור ומשדרת נחישות ועוצמה (לפחות כלפי פנים). עם זאת, לא ברור עד כמה

³⁷ Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 3

היא יעילה ועד כמה הציפיה שהיא מבטאת בת השגה³⁸ - על אחת כמה וכמה בהתחשב בכך שפעמים רבות, רטוריקה זו לוקה בחוסר בהירות מסוים³⁹.

באופן כללי, נראה שבקרב בכירים ואנשים שאינם בקיאים בתחום הסב"ר, רווחת התפיסה שאפשר ליישם את תאוריות ההרתעה הגרעינית על מרחב הסב"ר ללא שינויים נרחבים. אפשר שהדבר נובע מ"רקע תרבותי" כתוצאה מחייהם והכשרתם המקצועית בשלהי המלחמה הקרה ואפשר שהדבר נובע מהדמיון השטחי של אמל"ח הסב"ר לנשק גרעיני בהיבטי טווח, יכולת סיכול התקיפה ונזק פוטנציאלי.⁴¹ על פניו, אכן אפשר להקביל בין תקיפות בסב"ר לבין תקיפות גרעיניות. הנוזקות המסוגלות לפגוע בתשתיות חיוניות מסוגלות, לכאורה, להסב נזק רב בתוך זמן קצר ממרחק רב. כמו כן, האפשרות להגן נגדן קטנה⁴² והן מפותחות אך ורק על ידי מדינות בעלות יכולות גבוהות במיוחד - ולפיכך כמות השחקנים המחזיקה ביכולת זו מצומצמת. עם זאת, יש הטוענים שהקבלה זו היא שטחית - מכיוון שאמל"ח סב"ר "יחיד" אינו מסוגל להרס האדיר של אמל"ח גרעיני יחיד, אלא שעל פניו, נדרשת מערכה שלמה הכוללת תקיפת מערך נרחב של תשתיות חיוניות ומערכות אחרות לשם השגת תוצא קטסטרופלי.

אמל"ח סב"ר אינו מסוגל להבטיח תוצאים באותה רמת וודאות של נשק גרעיני, הן עקב הסתמכותו על פרצות שניתן לסגור והן עקב האופי הלא צפוי של מערכות מחשוב ומורכבותן הרבה. לבסוף, השימוש הצבאי בסב"ר הוא תיאורטי בעיקרו (בהיעדר דוגמה חיה), מסתמך על ספקולציות ואינו זוכה לאותה מידה של דיון ציבורי כפי שזכה לו הנשק הגרעיני (דיון ציבורי שייצב את ההרתעה הגרעינית ונתן לה מעמד מכונן בתפיסה של מקבלי ההחלטות). המאפיינים הללו של מרחב הסב"ר מחבלים ביכולת להשיג הרתעה יציבה בו ובאמצעותו ואפשר שההסתמכות על תפיסות של הרתעה גרעינית והתאמתן למרחב הסב"ר היא תוצאה של חוסר היכרות עם המרחב, פעולתו והיכולות הרלוונטיות בו - בדיוק כשם שבראשית העידן

³⁸ P. W. Singer, "How the United States Can Win the Cyberwar of the Future", *Foreign Policy*, 18 Dec. 2015,

<http://www.foreignpolicy.com/2015/12/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/>

³⁹ לראיה, נוסח סיכום וועדת נאט"ו בוולס, משנת 2014, קובע כי "הגנת סב"ר היא חלק ממטלות הליבה של נאט"ו בכל הנוגע לביטחון הקיבוצי. החלטה באשר למתי תקיפת סב"ר תוביל להפעלת סעיף 5 בתקבל על ידי המועצה הצפון אטלנטית, באופן בו ישקל כל מקרה לגופו". ראה:

Wales Summit Declaration, 05 Sept. 2014, www.nato.int/csp/en/natohq/official_text_112964.htm

⁴⁰ Patrick Cirenza, "The Flawed Analogy Between Nuclear and Cyber Deterrence", *Bulletin of the Atomic Scientists*, 22 Feb. 2016,

<http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179>

⁴¹ Patrick Cirenza, *An Evaluation of the Analogy Between Nuclear and Cyber Deterrence*, Stanford University, June 2015, pp. VI, 3-4

⁴² בהיעדר ניתוק מוחלט מהאינטרנט.

הגרעיני, תוארה ההרתעה הגרעינית באמצעות הסתמכות על תפיסות של כוח אווירי שנכתבו על ידי ג'וליו דואה וויליאם (בילי) מיטשל.⁴³

כאמור, התפיסה שאפשר להשיג הרתעה במרחב הסב"ר ושצריך לעשות זאת באמצעות שילוב של מניעה ושל ענישה נפוצה בקרב מדינות המערב.⁴⁴ בהתאם, אימצה ארה"ב מדיניות של הרתעה בסב"ר ובאמצעות הסב"ר כיעד במדיניות הביטחון הלאומי שלה.⁴⁵ ישנה אף תפיסה, שאליה שותף גם צבא היבשה האמריקני, לפיה אין הבדל בסיסי בין הרתעה במרחב הסב"ר לבין הרתעה בכל מרחב אחר. עם זאת, ניסיונות עבר של ארה"ב לנסח אסטרטגיית הרתעה ספציפית במרחב הסב"ר עלו בתוהו ובד בבד ישנה הבנה מסוימת לפיה, בהיעדר יכולות הגנה משמעותיות, אין יכולת לקיים הרתעה בסב"ר.⁴⁶ כמו כן, נראה שתפיסת ההרתעה בסב"ר אינה מוסכמה בינ"ל וגורמים סיניים, לדוגמה, טוענים כי אינה קיימת כלל. כראיה לפערי ההרתעה בסב"ר אפשר אף להביא את העובדה שעליונותה של ארה"ב בסב"ר אינה מרתיעה שחקנים – גדולים כקטנים – מלתקוף אותה במרחב זה.⁴⁷ לפיכך, הסתמכות על קיומה של הרתעה במרחב הסב"ר עשויה להביא לחישוב מוטעה ולהסלמה בלתי צפויה ונדרש מבט מעמיק יותר באתגרים ליישום אסטרטגיות הרתעה במרחב הסב"ר ובמענים הקיימים להם.⁴⁸

⁴³ Patrick Cirenza, "The Flawed Analogy Between Nuclear and Cyber Deterrence", *Bulletin of the Atomic Scientists*, 22 Feb. 2016,

<http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179>

⁴⁴ Liam Nevill, Zoe Hawkins, *Special Report: Deterrence in Cyberspace – Different Domain, Different Rules*, Berton Australia: Australia Strategic Policy Institute, July 2016, p. 7

⁴⁵ Clorinda Trujillo, *Op. cit.*, p. 44

⁴⁶ Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 7, 9

⁴⁷ P. W. Singer, *Op. cit.*

⁴⁸ Patrick Cirenza, "The Flawed Analogy Between Nuclear and Cyber Deterrence", *Bulletin of the Atomic Scientists*, 22 Feb. 2016,

<http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179>

פרק ג' – אתגרי ההרתעה בסב"ר

כאמור, ההרתעה היא נושא מעורר מחלוקת באופן כללי ומרחב מסב"ר הוא מרחב שהבנתו עדיין לוקה בחסר בקרב חוגים נרחבים של מקבלי החלטות. בשנים האחרונות רבה הכתיבה על נושא ההרתעה בסב"ר ועולות מגוון סוגיות המקשות על השגת ההרתעה בסב"ר. ואפשר לטעון שקיימים מספר תחומים עיקריים המגבילים את יכולת ההרתעה בסב"ר, ואלו הם כדלהלן:

חומרת הנזק וודאות

במרחב הסב"ר קיים כיום איזון ייחודי בין ההתקפה להגנה, השונה מזה הקיים במרחבים הפיזיים. על פניו, טכנולוגיית המידע פגיעה לחדירות מטבעה ובהינתן מצב זה, לתוקף ישנה עדיפות בכל הנוגע ליכולתו לחדור למערכות ולרשתות במרחב הסב"ר ולנצלן.

עם זאת, המצב מורכב יותר וישנם מספר גורמים הנותנים יתרונות מסוימים גם להגנה. ראשית, טכנולוגיית המידע אינה יוצרת תוצאים פיזיים באופן ישיר והיא נדרשת לתיווך של "טכנולוגיית הפעלה" (Operational Technology – OT)⁴⁹. ההפרדה בין המרחב "הלוגי" למרחב "הפיזי" (או בין טכנולוגיית המידע לטכנולוגיית הפעלה – OT/IT) והאיזוטריות היחסית של רבות ממערכות "טכנולוגיית הפעלה" מביאות לכך שכדי ליצור תוצאים פיזיים על ידי פעולה במרחב הסב"ר (לדוגמה- נזק פיזי לגנרטורים וכו), נדרשת השקעה ניכרת בכוח אדם מיומן, משאבים וזמן פיתוח. שנית, היכולת לתקן במהירות נקודות תורפה שהתגלו במרחב הסב"ר גורמים לכך שתהליך התקיפה באמצעות מרחב הסב"ר, גם אם לא להשגת תוצאים פיזיים, הוא ארוך ומורכב, מצריך מודיעין מדויק ושמירה על חשאיות לכל אורכו, עד להשגת התוצא, שכן כל גילוי של התקיפה יביא לסגירת התורפות שהיא הסתמכה עליהן ולכשלונה. נוסף על כך, אורך חיי האמל"ח עשוי להיות קצר, השימוש בו עשוי להיות חד פעמי – על אף המשאבים הניכרים שהושקעו בפיתוחו - ומכאן שהצורך לשמור על סודיותו יהיה רב. כך, שיטות התקיפה בסב"ר נטולות וודאות ומדינה יכולה להשקיע משאבים רבים בפיתוח יכולת מסוימת במרחב הסב"ר ולגלות, לעיתים ביום פקודה, שהיכולת כלל אינה עובדת, שהיריב גילה את הפרצה עליה הסתמכה היכולת וחסם אותה או שהיכולת התגלתה – לעיתים במקרה או אף על ידי צד שלישי.⁵⁰

מכאן, שכאשר מבקשים לפעול כדי לגרום לנזק קטן וחולף באמצעות מרחב הסב"ר, או כאשר רוצים לחדור למערכות לשם ריגול או למבצעי תודעה, מדובר במאמץ שאינו מורכב מאוד ביחס

⁴⁹ כגון מערכות שליטה תעשייתיות (ICS), מערכות פיקוח ואיסוף מידע (SCADA), מערכות שליטה מבוזרות (DCS) וכו.

⁵⁰ P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin, "Can Cyber Deterrence Work?", in: Andrew Nagorski (ed.), *Global Cyber Deterrence – Views from China, the US, Russia, India and Norway*, New York City, NY: The East-West Institute, April 2010, pp. 1-2

למבצעים מקבילים במרחב הפיזי ולתוקף יש עליונות על המגן. עם זאת, כאשר מבקשים לגרום לנזק פיזי ניכר באמצעות מרחב הסב"ר, מדובר בתהליך מורכב, ארוך ויקר פי כמה ביחס למרחב הפיסי.⁵¹

כיוון

במרחב הסב"ר גם אין אפשרות להגיע להשמדה הדדית **וודאית** (Mutual Assured Destruction), כפי שאפשר להשיג בתחומי הנשק הגרעיני ואף קשה, עד בלתי אפשרי, לשתק את כוחות הסב"ר של היריב, או אף לפגוע בהם באופן ניכר (אסטרטגיה הנקראת Counterforce). היעדר וודאות הנזק בסב"ר מצמצם מאוד את יכולת ההרתעה באמצעות הענישה בו ואף מקנה תמריץ לתקיפה בסב"ר – מתוך הנחה שמדובר בפעולה עליה הענישה, אם תתקיים, לא תהיה חמורה. זאת, בשילוב עם עליונות התקיפה על ההגנה מורידים את עלות התקיפה בסב"ר ומגדילים את התמריצים (והסיכוי) לתקיפה ראשונה באמצעות מרחב זה. מנגד, התמריץ לתקיפת תגובה בסב"ר יורד כיוון שהיא אינה מסוגלת לפגוע באופן משמעותי בתוקף ממילא (גם אם אפשר לזהותו – על אחת כמה וכמה אם מדובר בשחקן שאינו מדינתי) ואילו תקיפה קינטית בתגובה לתקיפה בסב"ר עשויה שלא להיות מידתית לנזק שנגרם. שילוב גורמים אלה מביא לשחיקה ביכולת ההרתעה על ידי ענישה.⁵²

כמו כן, כיוון שלתקיפה בסב"ר נדרש זמן הכנה ממושך ומודיעין מקיף, קשה יהיה להשתמש בתקיפות בסב"ר ככלי להרתעה תוך כדי עימות, או ככלי לתגובה אד-הוק. מכאן, קשה יהיה לקיים באמצעות הסב"ר הן הרתעה כללית (מפני כל תקיפה בסב"ר) והן הרתעה מיידיית (על תקיפות ספציפיות).⁵³

מאפיינים אלה גורמים לכך שאפשר שיכולת ההרתעה באמצעות ענישה במרחב הסב"ר אינה גדולה, כיוון שכל ניסיון לגרום באמצעותו לנזק משמעותי מסתמך על אמצעים יקרים לפיתוח, שהפעלתם אינה ודאית ושמשך הזמן מרגע ההחלטה על הפעולה ועד להשגת התוצא עשוי להיות ארוך. כך, אפשר שמרחב הסב"ר הוא מרחב שמטבעו נועד לפעולות קטנות, מתחת לסף התגובה, ולפעולות ריגול או תודעה, אך לא לשם הרתעה.

בהתאם, מרחב הסב"ר אכן נתפס כתגובה א-סימטרית לעוצמה הקונבנציונלית (והגרעינית) המערבית ומדינות מפתחות יכולות לפעול במרחב הסב"ר כדי לפצות על פערי עוצמה במרחבים הפיזיים. כך, רוסיה וסין בוחרות לפעול כנגד ארה"ב (ובעלות בריתה) דרך מרחב

⁵¹ Christopher A. Bartos, "Cyber Weapons are Not Created Equal", *USNI Proceedings Magazine*, Vol. 142/6/1, June 2016

⁵² Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 8; P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin, *Op. cit.*, pp. 1-2

⁵³ Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 10

הסב"ר כדי להימנע מהצורך להתמודד עם העוצמה הצבאית הקשה של ארה"ב.⁵⁴ משמע, מדינות אלה בונות על כך שפעולות במרחב הסב"ר נמצאות מתחת לסף התגובה הפיזי ומשתמשות במרחב זה כאמצעי לקזז את ההרתעה של היריב הנובעת מעוצמתו הפיזית. לפיכך, ליריבים חלשים יש תמריץ להשקיע ביכולות צבאיות במרחב הסב"ר ולהפעילן (בייחוד בהתחשב בפגיעות של מדינות המערב במרחב זה) ואילו למדינות מערביות יש תמריץ גדול יותר לפתח את כוחותיהם הקונבנציונליים ולהשקיע בהם.⁵⁵ במצב זה, אפשר ששחקנים חלשים דווקא יוכלו להרתיע בסב"ר שחקנים חזקים מהם.

ריבוי השחקנים במרחב והשונות בניהם

בעוד שההרתעה הגרעינית במלחמה הקרה שררה בעיקר בין שני צדדים – ארה"ב ובריה"מ⁵⁶ – כיום פועלים במרחב הסב"ר צדדים רבים מאוד. במרחב קיימים כיום מיליארדי משתמשים באופן כללי ואלפי שחקנים בעלי יכולות התקפיות בעלות משמעות זו או אחרת בפרט – חלקם מדינתיים וחלקם לא מדינתיים.⁵⁷ שיטות התקיפה במרחב הסב"ר רבות ומגוונות (הן במטרותיהן, ביעדיהן, בשיטות הביצוע ובנזק הנגרם מהן) גם הן, בעוד שההרתעה הגרעינית ואף הקונבנציונלית ניסו להרתיע מפני ביצוע מגוון מצומצם יחסית של פעולות. ריבוי שחקנים זה מביא להגדלת סיבוכיות אתגר ההרתעה בסב"ר, כיוון שהיא עשויה להידרש להיות יעילה לא רק נגד מעצמות שוות עוצמה או מדינות, אלא נגד מגוון רחב מאוד של יריבים לא מדינתיים בעלי מניעים, דרכי פעולה ודרכי חשיבה אחרות ומגוונות. לפיכך, המערכת במרחב הסב"ר מורכבת הרבה יותר מהמערכת הגרעינית הדו-קוטבית של המלחמה הקרה והדבר מקשה מאוד על השגת הרתעה. בהתאם, הרתעה במרחב הסב"ר עשויה להידמות יותר להרתעה של ארגוני טרור מאשר להרתעה באמצעות נשק גרעיני.⁵⁸

הצדדים השונים הפועלים במרחב הסב"ר אינם פגיעים לתקיפות בו באותה המידה. ישנם שחקנים במרחב החסינים יותר לענישה מאשר הגורמים המדינתיים כיוון שאינם מחזיקים בנכסים משמעותיים במרחב הפיזי נגדם אפשר לפעול, ואילו נכסיהם במרחב הסב"ר (חשבונות רשת חברתית, אתרי אינטרנט וכו') זולים וברי החלפה במהירות. מנגד, ענישה לא

⁵⁴ Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy", *Strategic Studies Quarterly*, Winter 2012, p. 110

⁵⁵ P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin, *Op. cit.*, pp. 1-2

⁵⁶ אומנם במלחמה הקרה גם בריטניה, צרפת וסין החזיקו בנשק גרעיני, אך מדובר היה במאגרים קטנים יותר וביכולות שיגור מוגבלות. עיקר "משחק ההרתעה" בתקופת המלחמה הקרה התנהל בין ארה"ב ובריה"מ.

⁵⁷ סוכנות בטחון הרשתות והמידע האירופאית (European Network and Information Security Agency – ENISA) מגדירה שישה סוגים של אימים על המדינה במרחב הסב"ר: תאגידים, גורמים פוליטיים, עובדים בשירות המדינה (Insider threat), פעילים פוליטיים (Hacktivists), מדינות וארגוני טרור. לכך מצרף מחקר של מרכז הסב"ר של נאט"ו שחקן נוסף והוא גורמים המופעלים על ידי מדינות (State Sponsored).

Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 3

⁵⁸ Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security*, Vol. 7 No. 1, 2014, p. 54; P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin, *Op. cit.*, April 2010, pp. 1-2

מדודה כנגד תשתיות בבעלות המדינה שבתוכה פועלים שחקנים אלה עשויה לגרום לתגובת נגד מצד המדינה שנגד שטחה, תשתיותיה או אזרחיה (גם אם לא נגדה) נערכה התגובה. בנוגע לשחקנים מדינתיים, מדינות מערביות, פתוחות ומקושרות תלויות הרבה יותר במרחב הסב"ר מחד גיסא ופגיעות בו הרבה יותר מאידך גיסא, ביחס ליריבותיהן. לפיכך, אפשר שיהיו למדינות שונות תמריצים לפעול במרחב הסב"ר עקב מידת הפגיעות של היריב, בעוד שליריב לא תהיה דרך להרתיע אותן באמצעות מרחב הסב"ר, או אף בכלל⁵⁹. זאת בשונה מהנשק הגרעיני או הקונבנציונלי, שמשפיע על כולם השפעה דומה⁶⁰. המגזר הפרטי משחק גם הוא תפקיד משמעותי במרחב הסב"ר ובכך מקשה על העברת מסר הרתעתי ברור, מביא לסיכויים משמעותיים לפגוע בשחקנים לא מעורבים חזקים וחשובים ועשוי אף לסייע (באופן עקיף או ישיר) לגורמים עוינים להגן על עצמם מתקיפה (לדוגמה – על ידי התלאת (Patching) שרת עליו יושב אתר של גורם עוין, מגינה חברה פרטית על אותו הגורם).⁶¹

חשאיות הפעולה במרחב והאמצעים לפעול בו

מרחב הסב"ר הוא מרחב בו "ערפל הקרב" סמיך ומקשה על התמצאות במרחב ועל מודעות מצבית בו באופן כללי. מאפיין זה של המרחב משפיע על יכולת ההרתעה במספר דרכים. ראשית, קיים קושי לגלות חלק נרחב מהחדירות למערכות מחשב. מאפיין זה של המרחב מתמרץ את היריב לתקוף בעצימות נמוכה ובתדירות גבוהה. כך, סיכוי סביר שהיריב יצליח לחדור באחד מניסיונותיו הרבים וסיכוי סביר שהחדירה – גם אם תתגלה – תמצא מתחת לסף התגובה לכשעצמה. הנפח הרב של ניסיונות התקיפה, הנערך במסגרת מערכה סדורה, יוצר תוצא מצטבר, אך הדרגתי, שלא אחת מצליח לעבור ללא תגובה ("אסטרטגיית הסלאמי"). גם אם המדינה הנתקפת בוחרת להגיב על החדירה למערכותיה, ככל שעובר זמן רב יותר בין ניסיון החדירה לבין התגובה עליו, הולך ופוחת התוצא המרתיע של התגובה ועשויה להיווצר מראית עין לפיה המדינה המגיבה עושה זאת באקראי, או אף היא התוקפנית בעצמה. לפיכך, בעיית גילוי החדירה חותרת תחת אמינות ההרתעה באמצעות ענישה של המדינה המרתיעה ואילו עצם החדירות הרבה של טכנולוגיית המידע, מקשה מאוד על הרתעה באמצעות מניעה.⁶² שנית, גם לאחר שאותרה התקיפה, קיים קושי בייחוסה לתוקף – הן עקב המגוון הנרחב של שחקנים הפועלים במרחב הסב"ר והן עקב קשיים טכניים. זאת בשונה מהוודאות בנוגע לגורם האחראי לתקיפה גרעינית או קונבנציונלית ומהמהירות היחסית שבמציאות האחראי לפעולה במקרים אלו. ראשית כל, המספר הגדול של שחקנים שונים, בעלי יעדים שונים ויכולות שונות,

⁵⁹ לדוגמה, אם תגובה במישורים הפיזיים תחשב כהסלמתית וחמורה מידי.

⁶⁰ וגם נשק זה, יש לציין, אינו יכול לשמש להרתעה כללית. לדוגמה, הוא אינו מרתיע ארגונים שאינם מדינתיים.

⁶¹ Liam Nevill, Zoe Hawkins, *Op. cit.*; P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin, *Op. cit.*, pp. 1-2

⁶² Liam Nevill, Zoe Hawkins, *Op. cit.*, pp. 9-14

הפועלים במרחב הסב"ר מקשה לייחס פעולות עוינות למקור ספציפי במידת ביטחון גבוהה.⁶³ שנית, התהליך הקיים לבירור זהותו של התוקף איטי ואינו בהכרח אמין, גם כאשר הוא מגיע לתוצאות. את סוגיית זיהוי התוקף במרחב הסב"ר אפשר לחלק לשלושה גורמים:

- זיהוי הארגון האחראי לתקיפה
- זיהוי המחשב או הרשת ממנה הגיעה התקיפה
- זיהוי האדם הספציפי (או האנשים הספציפיים) שתקף.

כל אחד מרמות זיהוי אלה מצריך אמצעים אחרים, משכי זמן אחרים ויעיל למטרות אחרות – כדי להפסיק תקיפות DDoS,⁶⁴ נדרש זיהוי שרתי הפיקוד והשליטה של הרשת התוקפת בזמן אמת, כדי להרתיע גורמים פוליטיים נדרש זיהוי של האדם התוקף הספציפי ואילו כדי להרתיע גורם מדינתי נדרש זיהוי של המקום ממנו הגיעה התקיפה והארגון העומד מאחוריה ולא בהכרח בזמן אמת.⁶⁵ מורכבות זיהוי התקיפה והתוקף מגדילה את הסיכויים שגם אם תתגלה החדירה, אי אפשר יהיה לייחס אותה לגורם ספציפי ולכן אי אפשר יהיה להענישו. התהליך הקיים יכול גם ליצור מצב שאכן ימצא התוקף, אך שאמינות שיזכו לתקיפה (או זהות שולחיו) תהיה נמוכה מידי בשביל תגובה או שיעבור זמן כה רב עד למציאתו, עד שיעילות התגובה תצטמצם. לבסוף, האופי חוצה הגבולות של התקיפות במרחב הסב"ר מביא ליכולת של התוקפים להתחמק מעונש עקב בעיות תיאום וסמכות בין גורמי האכיפה השונים – על אחת כמה וכמה אם אחריותם לתקיפה אינה וודאית. כך, עשויה להיווצר בעיה בנוגע למה לעשות לאחר שאותר התוקף - במיוחד אם המדינה שבשטחה הוא נמצא מסרבת לשתף פעולה בענישתו (בין אם מכיוון שהתוקף נשלח על ידה או שלא). לכן, עשוי להיווצר מצב בו המדינה הנפגעת תמאן להגיב, מחשש שתפגע בגורם שאינו אחראי לתקיפה ותיצור הסלמה. כמו כן, תקיפה חוזרת ונשנית כנגד גורמים שאינם מעורבים, עקב זיהוי מוטעה, עשויה להגדיל את התמריצים לתקוף במרחב הסב"ר בכל מקרה, כיוון ש"החפות" אינה משנה, אז "אם כבר נדרשים לשאת בעלות, לפחות להפיק מכך תועלת". כך, הגורם שאמור להרתיע, מורתע בעצמו והגורם שאמור להיות מורתע – הופך למרתיע.⁶⁶

במרחב הסב"ר, כמו במרחב הפיזי, זהות המטרה עומדת ביסוד היכולת לערוך תקיפה יעילה כנגדה – הן בהיבט הטכני (אילו מערכות יש לתקוף וכיצד) והן בהיבט הרעיוני (אילו סוגי

⁶³ Eric Sterner, "Retaliatory Deterrence in Cyberspace", *Strategic Studies Quarterly*, Spring 2011, p. 66
⁶⁴ Distributed Denial of Service – תקיפה בה השירות של רשת או רכיב בתוכה נפסק כיוון שהתוקף "הציף" אותה בתעבורה ממספר גדול של מקורות.

⁶⁵ David D. Clark, "Untangling Attribution", in: Committee on Deterring Cyberattacks, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, Washington, DC: National Research Council, 2010, pp. 25-26

⁶⁶ Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 11; Liam Nevill, Zoe Hawkins, *Op. cit.*, pp. 9-14; P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin, *Op. cit.*, April 2010, pp. 1-2

תוצאים יש לנסות ולהשיג) ולכן ליכולת שיוך התקיפה לתוקף יש חשיבות עצומה בקיום ההרתעה בסב"ר. בהיעדר היכולת לקבוע אחריות במידת ודאות גבוהה, קשה יהיה להצדיק תגובה בעוצמה רבה (ובייחוד כזו ברמה מקבילה ל"השמדה הוודאית ההדדית"). כך, חותר מאפיין זה תחת אמינות ההרתעה באמצעות ענישה.⁶⁷

אך זו אינה הבעיה היחידה. לשם הרתעה באמצעות ענישה, על המורתע לדעת מה הן יכולות המרתיע ולהבין את נכונותו להשתמש בהן. במרחב הפיזי הבהרות אלה נעשות הן באמצעות הצהרות, הן באמצעות הדגמות (תרגילים, ניסויים, מעורבות פומבית בלחימה ועוד) והן באמצעות בניין כוח גלוי. במרחב הסב"ר, קשה להעביר את חומרת האיום ואת אמינותו ליריב, כיוון שהפעילות במרחב מסווגת ברובה. אופי זה של הפעילות במרחב מחויבת המציאות, כפי שהוסבר לעיל, ואם יודגמו היכולות הקיימות בידי המדינה, עשוי הדבר לבטל לחלוטין את היכולות עליהן נשענת ההרתעה. מעטה הסודיות מגביל לא רק הדגמת יכולות פעילה, אלא אף הדגמה ברורה של בניין כוח בסב"ר וכך, בשונה מיכולות מוסכמיות או גרעיניות, בניית יכולות פעולה בסב"ר עשויה שלא להיתרגם להרתעה, כיוון שהאויב אינו מודע לה או לפרטיה. החשאיות הכרוכה במרחב הסב"ר גם מקשה את השימוש באמצעים הקלאסיים לבניית אמון (Confidence Building Measures) כגון משקיפים והודעה מראש על הפעלת אמצעים ופעולות במרחב הסב"ר – דבר שמוסיף ומקשה על השגת הרתעה מבחינת נראות האמצעים ואף מגדיל את הסיכוי להסלמה – מכוונת או שאינה מכוונת - עקב הפעלתם או כמכת מנע להפעלתם. שיטות התקיפה בסב"ר ניתנות לשימוש על ידי האויב מרגע שהתגלו. לא זו אף זו, "ההנדסה ההפוכה" של שיטות אלה וניצולן על ידי גורמים אחרים (או אף יריבים) עשויות להיות זולות ופשוטות הרבה יותר מאשר מלאכת פיתוח השיטות מלכתחילה. לפיכך, כל פעולה במרחב הסב"ר עשויה דווקא להגדיל את הפגיעות של היזם ואת היכולות של יריביו. אך בהיעדר הדגמת יכולות כל שהן, התועלת הנובעת מהכרזות תקיפות בלבד מוגבלת.⁶⁸

גם בהינתן תגובה לתקיפה בסב"ר שאינה בבחינת "הדגמת יכולות", פרסומה יהיה בעייתית מאותן הסיבות של חשיפת מקורות ושיטות פעולה ועשויה להביא לביטול היכולת לערוך תקיפות דומות לא רק נגד התוקפן הספציפי, אלא נגד שחקנים אחרים אותם אפשר היה לתקוף בעתיד באותו הערוץ, לו היה נשאר חסוי. האופי החשאי של הפעולות במרחב הסב"ר יקשה גם לספק את הרצון הציבורי (והצורך הפסיכולוגי הן של התוקף והן של המגיב) לתגובה מהירה והחלטית. מכאן שעצם התועלת בתגובה בסב"ר עשויה להיות מצומצמת כי אם תקיפת הנגד לא פורסמה, הרי שערכה ההרתעתי אינו קיים.⁶⁹ מנגד, תגובה "קינטית" מחוץ למרחב

⁶⁷ Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 11; Liam Nevill, Zoe Hawkins, *Op. cit.*, 9-14; P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin, *Op. cit.*, pp. 1-2

⁶⁸ P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin, *Op. cit.*, pp. 1-2

⁶⁹ P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin, *Op. cit.*, pp. 1-2

הסב"ר היא בעייתית עקב היעדר תקדימים והבעייתיות (המנטלית והנורמטיבית) בלגרם נזק פיזי בתגובה על נזק שאינו פיזי. תגובה שאינה קינטית מחוץ למרחב הסב"ר (סנקציות כלכליות, דיפלומטיות או משפטיות) עשויה להיות בלתי מידתית לתקיפה או להיות איטית מידי בהשפעתה וכך לא מרתיעה.⁷⁰

הסיכון להסלמה והיעדר הנורמות הבין לאומיות

אפשר שאחד הפערים המרכזיים בהרתעה בסב"ר הוא היעדר אמות המידה והנורמות הבינ"ל. הרתעה באמצעות ענישה מחייבת הצבת סף ברור ("קו אדום") בין התנהגות מקובלת לבין התנהגות לא מקובלת. מצב זה גורם לכך שאין תפיסה אחידה בנוגע לאילו מעשים עוינים במרחב הסב"ר ופגיעה באלו סוגי מטרות נחשבים מעשה תוקפנות בסב"ר, באיזו עוצמה יש להגיב למעשים כאלה ובאילו כלים. הבעיה אינה כל כך במצבי הקיצון, אלא בעיקר במצבי הביניים והמינוח הקיים אינו מסייע להבהרת הקווים האדומים. לדוגמה, מעשי גניבה וריגול הם פעולות שאינן נחשבות לפעולה לוחמתית במרחב הפיזי ולא מחייבות תגובה של המדינה לשם ביסוס ההרתעה. עם זאת, בעוד שבמרחב הפיזי, תקיפה כוללת אך ורק נזק לרכוש או לחיי אדם, כמעט כל מעשה עוין במרחב הסב"ר מכונה "תקיפה". זאת מכיוון שבמרחב הסב"ר, פריצה לשם ריגול או גניבה (שמוסכם שאינם פעולה לוחמתית, אלא פעולה מקובלת) עשויה לשרת (בו-זמנית, או לאחר מכן) כוונתור לתקיפה. עוד, לא ברור האם שימוש במרחב הסב"ר לצורך מבצעי "תודעה" הוא מעשה תוקפנות וכיצד יש להגיב עליו. כמו כן, הקו בין פשיעה בסב"ר ותקיפה צבאית בסב"ר עשוי להיות מטושטש, עד כדי לא קיים כלל. כך לדוגמה, תקיפה של בנק על ידי ארגון פשע עשוי להיות מונע הן ממניעים כלכליים והן ממניעים מדיניים ולהיעשות אף על ידי שחקנים הפועלים בשירות, ישיר או עקיף, של מדינה. ההבחנה בין אלה לאלה קשה וכך גם ההחלטה כנגד מי להגיב וכיצד.⁷¹ לכן, פוטנציאל סף התגובה עשוי להיות נמוך מכדי יישום של הרתעה באמצעות ענישה על פעולות עוינות רבות במרחב הסב"ר.⁷² יש הטוענים שעל פיתוח הנורמות והכללים לפעולה בסב"ר להיעשות הן במסגרות בין לאומיות (על ידי אמנות) והן במסגרות פנים לאומיות (על ידי חקיקה).⁷³ עם זאת, גיבוש נורמות ברורות

⁷⁰ Liam Nevill, Zoe Hawkins, *Op. cit.*, pp. 9-14; Danny Vinik, "America's Secret Arsenal", *Politico*, 10.12.2015, <http://www.politico.com/2015/12/defense-department-cyber-offense-strategy-000331>

⁷¹ P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin, *Op. cit.*, April 2010, pp. 1-2

⁷² Liam Nevill, Zoe Hawkins, *Special Report: Deterrence in Cyberspace – Different Domain, Different Rules*, Berton Australia: Australia Strategic Policy Institute, July 2016, pp. 9-14

⁷³ Tang Lan and Zhang Xin, *Op. cit.*, pp. 2; Liam Nevill, Zoe Hawkins, *Op. cit.*, pp. 16-18; Dmitry I. Grigoriev, "Russian Priorities and Steps Towards Cybersecurity", in: Andrew Nagorski (ed.), *Global Cyber Deterrence – Views from China, the US, Russia, India and Norway*, New York City, NY: The East-West Institute, April 2010, pp. 5-7; Pavan Duggal, "Cyber Deterrence: Legal Perspectives", in: Andrew Nagorski (ed.), *Global Cyber Deterrence – Views from China, the US, Russia, India and Norway*, New York City, NY: The East-West Institute, April 2010, p. 9; Stein Schjolberg, "Wanted: A

וסף ברור בין התנהגות מקובלת לכזו שאינה מקובלת הוא מלאכה לא פשוטה, כיוון שיש מדינות שמטרתן לדכא התנגדות פנימית וחופש ביטוי באמצעות מרחב הסב"ר, ואילו יש מדינות המחויבות יותר לחופש ביטוי ולניטרליות רשת. הבדלים אידיאולוגיים אלה בקשר לאופי המרחב יקשו גם להגיע להרתעת יריבים "לא דמוקרטיים" המתבססת על ערכים.⁷⁴ כמו כן, במידה רבה, למדינות השונות יש אינטרס להימנע מהרתעת יתר כנגד פעולות במרחב הסב"ר ולשמר את הלגיטימיות של תקיפות במרחב הסב"ר, זאת משום שמדינות רבות – ובמיוחד המעצמות – משתמשות במרחב הסב"ר ככלי לפעולות עוינות הנתפסות כלגיטימיות בין מדינות – לדוגמה, ריגול (צבאי, פוליטי או תעשייתי) או מבצעי הונאה והשפעה, עקב התועלת הרבה והמחיר הנמוך (יחסית) של תקיפות שכאלה – בין אם בשגרה ובין אם בחירום. יצירת הרתעה ברורה כנגד פעולות עוינות במרחב הסב"ר עשויה לחבל ביכולתן להשתמש במרחב זה. מכאן, אין לשחקנים אלה אינטרס להגיב באופן תקיף ותוקפני מידי על התקפות במרחב הסב"ר, בין השאר כדי לא לקבוע נורמה בתחום, ואילו העובדה ששחקנים רבים תוקפים במרחב הסב"ר גורמים לכך שתקיפות אלה מקבלות בהדרגה סוג של לגיטימיות.⁷⁵ לפיכך, האקלים הנורמטיבי כיום לא רק שאינו בהכרח מרתיע מפני תקיפות במרחב הסב"ר, אלא אולי הוא אף מעודד אותן. אם נרצה, נוכל להשוות זאת לשימוש בנשק להשמדה המונית (ועל אחת כמה וכמה השימוש בנשק גרעיני), שנתפס כמעשה פסול עד כדי טאבו בקרב הקהילה הבינ"ל.⁷⁶

ככל ניסיון ענישה, גם במרחב הסב"ר מסתכן המגיב בהסלמה של העימות. עם זאת, עקב האופי הבלתי צפוי של "אמצעי הלחימה" המופעלים במרחב הסב"ר, מרגע שהכריז המרתיע על מדיניות של הרתעה באמצעות ענישה בסב"ר, הרי הוא מסתכן באובדן אמינות (וכך, בשחיקת ההרתעה) במקרה שבחר שלא לממש את איומיו או שלא יצליח לעשות זאת. בהינתן מאפייני מרחב הסב"ר שנסקרו לעיל והקשיים שהם משיתים על הענישה, אפשר שההכרזה מראש על מדיניות הרתעתית באמצעות ענישה אינה מועילה כלל ואילו היעדר ההכרזה על מדיניות ענישה, חותרת תחת יסודות התפיסה.⁷⁷

מנגד, להרתעה במרחב הסב"ר ודרך מרחב הסב"ר יש בעיה ערכית נוספת בכל הנוגע למעבר בין פעולה במרחב זה לבין פעולה במרחבים הפיזיים. כך, נשאלת השאלה על אילו פעולות במרחב הסב"ר תגיב המדינה במרחבים הפיזיים ובאיזו עוצמה. שאלה זו נוגעת בליבת הסוגיה של על מה שווה להסתכן בהסלמה, שעשויה אף להגיע עד כדי מלחמה גרעינית במקרה של

'United Nations Cyberspace Treaty', in: Andrew Nagorski (ed.), *Global Cyber Deterrence – Views from China, the US, Russia, India and Norway*, New York City, NY: The East-West Institute, April 2010, p. 11

⁷⁴ Liam Nevill, Zoe Hawkins, *Op. cit.*, pp. 9-14

⁷⁵ Clorinda Trujillo, *Op. cit.*, p. 49

⁷⁶ P. W. Singer, *Op. cit.*; Clorinda Trujillo, *Op. cit.*, p. 47-48; Tang Lan and Zhang Xin *Op. cit.*, pp. 1-2

⁷⁷ Liam Nevill, Zoe Hawkins, *Op. cit.*, pp. 9-14

הסלמה בין מעצמתית. כך, אפשר לראות שאפילו במקרים בהם הפגיעה דרך מרחב הסב"ר נתפסת כחמורה ואפילו כאשר זהות התוקפן ברורה בודאות רבה יחסית, כגון בכל הנוגע להתערבות הרוסית במערכת הבחירות האמריקנית של שנת 2016, אז סוכנויות המודיעין של ארה"ב הצביעו בפומבי על רוסיה כעל הגורם האחראי, עדיין לא התרחשה תגובה תקיפה במרחבים הפיזיים.⁷⁸ במקרה זה, אפשר שהתרחש מצב של הרתעה הדדית, בו ההרתעה מפני מלחמה, שעשויה להפוך למלחמה גרעינית, הרתיעה את האמריקנים מתגובה לפעולות הרוסיות – וזאת למרות השלכות שליליות אפשריות לתדמית האמריקנית בכלל. כך, נפתח מרחב בו הרוסים היו למעשה יכולים לפעול, אפשר שביעילות רבה ותוך השגת הישגים ניכרים, מתחת לסף התגובה האמריקנית. לפיכך, אפשר שאם מגמה זו תמשיך, יתקבע מצב⁷⁹ בו התגובה לפעולות במרחב הסב"ר תהיה בעיקר באמצעות מרחב הסב"ר. לחילופין, אפשר שהתגובה תתחלק לתגובה גלויה וסמלית (כדוגמת סנקציות) ולתגובה חשאית משמעותית יותר, שתפגע ביריב, אך לא תחייב הסלמה נוספת.⁸⁰ עם זאת, מידת ההרתעה של התגובה החשאית עשויה להיות מוגבלת, כיוון שלהרתעה יש יסוד תודעתי המחייב נראות.⁸¹ כך, גם אם תגובה חשאית לחיזוק ההרתעה תוכל להרתיע את מושא התגובה מהמשך פעולתו, היא לא תוכל להרתיע צד שלישי. צד שלישי זה עשוי אף לטעות בחישוביו ממה שנדמה כהיעדר תגובה על הפגיעה ולהסיק שהוא יוכל לערוך מבצעי סב"ר ללא חשש – דבר שעשוי להגדיל את סיכויי הפעולה העוינת, את היקף הנזק שלה ואת סיכויי ההסלמה בעקבותיה. לבסוף, תגובה חשאית עשויה לשחוק את האמינות של השחקן המגיב כלפי גורמים ידידותיים ואחרים, כיוון שהוא עשוי להיתפס כלא החלטי ואף כמורתע בעצמו.⁸²

האתגרים שפורטו לעיל, ובייחוד הסודיות הגדולה האופפת את כל העיסוק הביטחוני בסב"ר גורמת לפער ידע ופערי הבנה משמעותיים בנוגע לאופן בו מתנהל המעשה הצבאי במימד זה ובכל הנוגע להשפעתו. פערי ידע אלה מתחדדים בהתחשב בכך שמדובר תחום חדש לגמרי.

⁷⁸ Susan Hennessey, "Is US Cyber Deterrence Strategy More than (Russian) Roulette?" *Lawfare*, 12 Oct. 2016

⁷⁹ הממשל האמריקני כבר הבטיח תגובה מידתית, שעשויה להיות חשאית, הן על מבצעי הסב"ר שנערכו במהלך מערכת הבחירות האמריקנית, הן על הפריצה למערכות המשרד לניהול כוח אדם הפדרלי (OPM) והן לפריצה למערכות של חברת סוני (Sony Entertainment).

⁸⁰ *Ibid*

⁸¹ Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy", *Strategic Studies Quarterly*, Winter 2012, p. 101, 107

כך, לדוגמה, במהלך תקופת קרטר, הדליפו האמריקנים את עיקרי "החלטה נשיאותית 59" (Presidential Directive 59) שעיקרה היה ההחלטה לאיים בנשק גרעיני על מה שנתפס בווייטנאם כשילוש האינטרסים הסובייטי הבסיסי – שרידות בכירי הממשל הסובייטי עצמם, שרידות המשטר הסובייטי ואחיזתו של המשטר באירופה. המטרה של החלטה זו הייתה לחזק את ההרתעה הגרעינית האמריקנית, אל מול מה שנתפס כשחיקה.

John G. Hines, Ellis M. Mishulovich, John F. Shull, *Soviet Intentions 1965-1985 Vol. 1 – An Analytical Comparison of US-Soviet Assessments During the Cold War*, Mclean, VA: BDM Federal Inc. (for OSD-Office of Net Assessment), 22 Sept. 1995, p. 15

⁸² Susan Hennessey, *Op. cit.*

לפיכך, אי הידיעה וההבנה גדולים משמעותית גם ביחס לתחומים סודיים אחרים כגון כוחות מיוחדים.⁸³ אי ההבנה ואי הידיעה - במיוחד בקרב מקבלי ההחלטות - עשויים להשפיע על ההרתעה של איומים הקשורים במרחב הסב"ר. השפעה זו יכולה להתבטא בהגדלת פוטנציאל ההרתעה של האיום או בהקטנתו ופועלת הן על המרתיע והן על המורתע.. כך, מחד גיסא, חוסר הוודאות הטבוע בהשפעה של כלי הסב"ר, אי הוודאות הכללית יותר בנוגע להאם להגיב בסב"ר או במרחבים הפיזיים (או גם וגם), מה תגובה שכזו תכלול, כיצד היא תעמוד באמות מידה משפטיות, מוסריות וציבוריות, כיצד היא תתפרש בצד השני, איזו תגובת-נגד היא תביא, באילו מרחבים ועוצמות תיערך תגובת הנגד וכו'⁸⁴ עשויים להרתיע מפני השימוש בהם.⁸⁵ מאידך גיסא, ככל שהשימוש ההתקפי\איסופי במרחב הסב"ר יגדל, כך תגדל מידת הביטחון של מקבלי ההחלטות בכלים אלה (ומידת היכרותם עם המרחב) ובהתאם, תקטן ההרתעה העצמית מפני ניצולו של מרחב זה ופעולה בו. מכאן שנושא ההרתעה, שמלא בסימני שאלה לכשעצמו, הופך למורכב ומסובך אף יותר כאשר הוא נוגע למרחב הסב"ר.

פרק ד' – מימוש ההרתעה בסב"ר

על אף האתגרים הכרוכים בהרתעה בסב"ר, אפשר שהעליונות של ההתקפה על ההגנה במרחב הסב"ר מחייבת שימוש בהרתעה, כדי לצמצם עד כמה שאפשר את ההתקפות, את היקפן ואת השלכותיהן.⁸⁶ הרתעה זו שונה במספר מובנים מאשר ההרתעה הגרעינית או

⁸³ Danny Vinik, "America's Secret Arsenal", *Politico*, 10.12.2015,

<http://www.politico.com/2015/12/defense-department-cyber-offense-strategy-000331>

⁸⁴ שכן, אפשר שהיריב תיקן בהחבא את הפגיעות עליה הסתמכה תקיפת סב"ר כלשהי וכך הפך אותה, ללא ידיעת התוקף, לבלתי יעילה לחלוטין.

⁸⁵ Danny Vinik, *Op. cit.*; Leo Miri, "Worrying About Cyber War Is Making Us Less Safe", *Defense One*, 3 Dec. 2014,

<http://www.defenseone.com/technology/2014/12/worryinh-about-cyber-war-making-us-less-safe/100424/>

⁸⁶ Laura K. Bate, "In Search of Cyber Deterrence", *War on the Rocks*, 24 Sept. 2015,

www.warontherocks.com/2015/09/in-search-of-cyber-deterrence

הרתעה אחרת במרחב הפיזי. באופן כללי, כדי להשיג הרתעה במרחב הסב"ר, נדרשים המרכיבים הבאים:⁸⁷

- בהירות: היכולת להעביר באופן ברור ליריבים בפרט ולקהיליה הבינ"ל בכלל מה הם הפעולות המתקבלות על הדעת במרחב הסב"ר ומה הם הקווים האדומים שיגרמו לתגובה. במרחב הסב"ר, לבהירות המסר תפקיד משמעותי כיוון שאי-הבהירות היא מאפיין מובנה של הסביבה. בהירות נדרשת לא רק בהבהרת הקווים האדומים, אלא בהבהרת התגובה להפרתם – הן לפני הוצאתה אל הפועל, תוך כדי התגובה ולאחר מכן – כדי להגביל את אי ההבנה ואת הסיכוי להסלמה בלתי נשלטת.
- אמינות: על היריב להאמין שהמדינה תוציא אל הפועל את האיומים שפרסמה כתגובה על הפעולות שהיא מעוניינת להרתיע.
- יכולת זיהוי ושיוך ((Attribution): נדרשת היכולת לזהות את הפעולה העוינת במרחב זה ולשייך אותה באופן אמין מספיק לשחקן ספציפי (גם אם לא לאדם ספציפי). שיוך הפעולה נדרש לא רק לזהות את המקור הגיאוגרפי של התקיפה, אלא גם לאמוד באיזו מידה הייתה המדינה ממנה התרחשה התקיפה (או השחקן הלא מדינתי) מעורבת בה – האם התקיפה נעשתה בידיעת המדינה, בהכוונתה, על ידה, באישורה או שמא ללא כל מעורבות מצידה.
- מידתיות: יש צורך להכריע עד כמה נדרשת התגובה להיות מידתית לפעולה אותה היא נדרשת להרתיע. סוגיית המידתיות נוגעת גם לשאלות האם על התגובה להישאר במרחב הסב"ר, או שמא להתרחש מחוצה לו והאם עליה להיות קינטית באופייה או בתוצאה. במסגרת העיסוק בסוגיית המידתיות נדרשת בחינה הן באופן בו תמנע הסלמה והן בצמצום הנזק האגבי.

המורכבות של סוגיית ההרתעה בסב"ר כפי שפורטה לעיל, גורמת לכך שניהול התגובה יהיה פעולה עדינה מאוד. כיוון שההרתעה בסב"ר כוללת מגוון נרחב של כלים ושחקנים והיא מתמשכת (כיוון שכשולן אינו מסתיים בהשמדה כוללת), היא מורכבת יותר ולכן מצריכה תהליכי חשיבה ומשחקי מלחמה מעמיקים ונרחבים. זאת בשונה מסוגיית ההרתעה הגרעינית שלרוב דנה אך ורק בשני צעדים (תקיפה ראשונה ושנייה).⁸⁸ דוגמה למורכבות הסוגיה אפשר לראות במאמצי התגובה של ארה"ב לתקיפות שנערכו נגדה במרחב הסב"ר. במאמץ לשפר את יכולת ההרתעה האמריקנית, חתם הנשיא אובמה בחודש אפריל 2015 על צו נשיאותי שיאפשר לשר האוצר, תוך התייעצות עם שר המשפטים ועם מזכיר המדינה, להטיל סנקציות

⁸⁷ Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security*, Vol. 7 No. 1, 2014, pp. 56-60; Laura K. Bate, "In Search of Cyber Deterrence", *War on the Rocks*, 24 Sept. 2015, www.warontherocks.com/2015/09/in-search-of-cyber-deterrence

⁸⁸ P. W. Singer, *Op. cit.*

אישיות⁸⁹ על כל אדם המעורב (באופן ישיר או עקיף) בהתקפות במרחב הסב"ר (או דרכו) כנגד ארה"ב (כל עוד מקור התקפות אלה נמצא מחוץ לגבולות ארה"ב) או ארגון שנמצא בבעלותה – כולל קבלה של כספים או קניין רוחני שמקורותיהם מפעולה בלתי חוקית כנגד ארה"ב במרחב הסב"ר.⁹⁰ מטרת הסנקציות האלה הן הרתעה באמצעות ענישה אישית של גורמים עוינים במרחב הסב"ר. הניסיון לפעול באופן כלכלי כנגד יחידים וארגונים בבעלותם, כמו גם הסמכות לפעול כנגד כל מי שמעורב באופן זה או אחר בפעולה⁹¹ מצביע על המנעד הרחב של הגורמים אותם יש להרתיע במרחב הסב"ר – החל מפצחנים יחידים, דרך חברות המנסות לבצע ריגול תעשייתי וכלה במדינות. עם זאת, כיוון שקשה למצוא את האנשים הספציפיים שביצעו את הפעולה, מנסה הצו לאפשר לנקוט סנקציות נגד כל מי שקשור לפעולה, גם באופן עקיף, וכמו כן נגד כל צד שלישי העשוי להרוויח מהפעולה באופן ישיר. כך, אם מבצעים הפעולה עצמם לא יורתעו, הכוונה היא להרתיע גורמים שונים שסייעו להם, אפילו ללא כוונת זדון (כגון ספקי שירותי IT שונים – מספקי אינטרנט ועד ספקי איכסון ושרתים). הרתעה זו אמורה להתאים לא רק להרתעת ארגונים ויחידים אלא גם להרתעת גורמים מדינתיים, בדומה לדפוס התנהלות האמריקנית בעת האחרונה נגד רוסיה, שבין השאר הטילה סנקציות אישיות כנגד בכירים ברוסיה ובכירים לשעבר באוקראינה בתגובה על פעולותיה של רוסיה כנגד אוקראינה.⁹² מנגד, בד בבד, אמור הצו לא לשמש ענישה חמורה עד כדי הסלמה למלחמה ולכן לא להטיל סנקציות מדינתיות נרחבות, שכן לעיתים קרובות אין אפשרות להוכיח באופן ישיר אחריות מדינתית לפעולה במרחב הסב"ר.

אפשר שמענה מסוים לסוגיית ההרתעה בסב"ר יכיל את הנקודות הבאות, כדלהלן.

הרתעה באמצעות מניעה

רבים מהאתגרים שפורטו לעיל משפיעים באופן מיוחד על ההרתעה באמצעות ענישה. מכאן, אפשר אפשר שהקשיים הללו מגדילים את הצורך לבחור באסטרטגיות הרתעתיות אחרות, בעיקר מניעה.⁹³ את ההרתעה באמצעות מניעה בסב"ר אפשר לחלק לשני חלקים – הגנה

⁸⁹ המתבטאות בהקפאת נכסים בארה"ב.

⁹⁰ Executive Order – "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", 01 Apr. 2015,

⁹¹ הצו מאפשר להטיל סנקציות נגד מבצעי הפעולה עצמם, גורמים המשתפים עימם פעולה או מסייעים להם, גורמים המרוויחים מהפעולה באמצעות קבלת יתרון או רווח כלכלי וכל גורם הנשלט על ידיהם או הפועל למענם או בשמם.

⁹² בהתאם ראה:

Andrew S. Swiss, Richard Nephew, *The Role of Sanctions in US-Russian Relations*, Carnegie Endowment for International Peace, 11 Jul. 2016,

www.carnegieendowment.org/2016/07/11/role-of-sanctions-in-u.s.-russian-relations-pub-64056

⁹³Liam Nevill, Zoe Hawkins, *Op. cit.*, pp. 15-1, 19

ואיתנות. תפקיד ההגנה להרתיע מתקיפה על ידי הגבלת יכולת התקיפה, צמצום סיכויים הצלחתה והגדלת מחירה. מנגד, תפקיד האיתנות להרתיע מתקיפה על ידי צמצום התועלת שבה והגדלת אמינות התגובה עליה.⁹⁴ בכך, יש המשווים את ההרתעה בסב"ר למערכת הקיימת העוסקת בבטיחות או בבריאות הציבור, שמטרתה להגדיל את איתנות החברה, המדינה ומנגנוניה וכך להגן עליהן ולא בהכרח להרתיע באמצעות עונש.⁹⁵

המניעה תעשה על ידי חיזוק ההגנות במרחב הסב"ר, יכולת ההתראה על תקיפות, איתנות הרשתות והתשתיות החיוניות המסתמכות עליהן, יכולת השיקום המהיר והיתירות במרחב זה. יכולות אלה ישפיעו על מערך החישובים של האויב כיוון שהפגיעה שיצליח לגרום עשויה שלא להיות קשה כפי שהוא מעוניין ואילו יכולת הנפגע להגיב תישמר.⁹⁶ כך, יידרש מהיריב מאמץ רב יותר כדי לחדור למערכות אליהן הוא ירצה לחדור ואילו התועלת הנובעת ממאמציו תצטמצם. הרתעה זו דומה במידת מה להתרעה על ידי מכה שנייה של המלחמה הקרה, עם זאת, בשונה מאשר רוב התקיפות בסב"ר, כנגד מכה גרעינית אי אפשר היה לקיים יכולת התאוששות מהירה. קיום יכולת התאוששות מהירה בנוסף לאיתנות וליכולת "מכה שנייה" עשויה להוסיף לאמינות ההרתעה באמצעות מניעה. גישה זו עשויה שלא להספיק להרתעת השחקנים החזקים הפועלים במרחב הסב"ר והיא אף נוטה להיות סבילה במהותה ולוותר על היוזמה לטובת התוקף, אך לכל הפחות, היא תאפשר לצמצם את נפח התקיפות הכולל על הרשת על ידי הנאת השחקנים החלשים מלעשות זאת – וכך, יאפשר למדינה להתרכז בהתמודדות נגד השחקנים החזקים יותר.⁹⁷

בהיבטי חיזוק ההגנה, קיימת גם סוגיית האחריות האישית. יש הטוענים שלעיתים קרובות, מערכות נכשלות כיוון שהאחראים עליהן אינם נושאים במחיר הכישלון – ולפיכך אין להם תמריץ למנוע אותו. בהתאם, אפשר שחלק מההרתעה הנדרשת בסב"ר היא דווקא הרתעה "פנימית" – כלומר, הרתעת המגן⁹⁸ מפני כישלון בתפקידו. הרעיון הוא ליצור תמריץ גדול ככל האפשר אצל המגן לשפר את הגנותיו, גם בהינתן עלויות כלכליות ואחרות הכרוכות בכך.⁹⁹ במערכות אזרחיות אפשר לעשות זאת על ידי תיקון החוקים והתקנות הקיימים כך שיטילו

⁹⁴ Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 9

⁹⁵ Eric Sterner, "Retaliatory Deterrence in Cyberspace", *Strategic Studies Quarterly*, Spring 2011, p. 67

⁹⁶ P. W. Singer, *Op. cit.*,

⁹⁷ Liam Nevill, Zoe Hawkins, *Op. cit.*, pp. 15-1, 19

⁹⁸ יש לציין שלא ברור מי הוא "המגן" – האם מדובר בחברה המפתחת את התוכנה או החומרה או שמא בחברה המפעילה אותם? כמו כן, בהינתן העובדה שטכנולוגיית המידע פגיעה באופן מובנה והקשרים ההדוקים בין החומרה, התוכנה וההפעלה, קשה יהיה להטיל אחריות על כל אחד מהגורמים הללו באופן נפרד, או אף על כולם ביחד.

⁹⁹ Tyler Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options", in: Committee on Deterring Cyberattacks, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, Washington, DC: National Research Council, 2010, p. 4

אחריות לכישלון על גורמים שונים העוסקים בהגנת הרשתות. אחריות זו אינה חייבת להיות פלילית, אלא היא יכולה להיות גם אזרחית או אף ציבורית.¹⁰⁰

הגדלת יכולת ההגנה והאיתנות¹⁰¹ בסב"ר היא מאמץ נרחב ורב משתתפים, המחייב הירתמות, שיתוף פעולה ויכולות טכניות של מגוון רחב של שחקנים – גדולים כקטנים, עד לאזרח הפשוט. זאת מכיוון שאחד מהמאפיינים של מרחב הסב"ר הוא קשרי הגומלין הענפים (והמורכבים) הקיימים בו. עקב כך, כל מדינה וכל גוף בתוך המדינה נדרש להגן בעצמו על עצמו ועל רשתותיו במרחב הסב"ר - זאת מכיוון שהגנה על רשתותיו של גוף אחר מצריכה פתיחה מוחלטת שלהן בפני "צד שלישי" ומביאה לפגיעות רבה ולסוגיות ביטחון מידע ופרטיות.¹⁰² עם זאת, ישנה גם מידה רבה של תלות הדדית, המאפשרת אגבור של מאמצי הגנה של גורמים שונים. לדוגמה, כיוון שהרשת הצבאית והממשלתית תלויות ברשת האזרחית הפרטית (לדוגמה, כאשר פריצה לספקי משנה עשויה לאפשר פריצה לרשת הצבאית או הממשלתית), שיפור ההגנה על הרשת האזרחית תשפר את ההגנה על הרשת כולה וכך תשפר, אולי, גם את ההרתעה העקיפה. יש אף הטוענים שקשרי הגומלין בסב"ר עשויים לגרום לכך שתקיפה בו או דרכו תגרום נזק רב הן לתוקף והן לנתקף. נזק זה עשוי לכשעצמו להיות גדול במידה שתרתיע את התוקף מלבצע את התקיפה. כך, אפשר שהידוק קשרי גומלין של רכיבים מסוימים במרחב הסב"ר עשויים לשמש כחלק מאסטרטגיית הרתעה.¹⁰³

כך או כך, ברור שהרתעה על ידי מניעה לעולם אינה עומדת לבדה ונדרשת גם הרתעה באמצעות ענישה (וההיפך). מכאן שבצד חיזוק ההגנה והאיתנות, על המדינה להבהיר במעשיה ובהכרזותיה שהיא תנקוט בפעולות תקיפות על מנת להבטיח את האינטרסים שלה במרחב הסב"ר.¹⁰⁴

סוג כזה של הרתעה באמצעות מניעה היא ה"הרתעה המותאמת" (Tailored Deterrence). הרתעה שכזו אמורה להגדיל את עלויות תקיפות הסב"ר של היריב ולצמצם את התועלת הנובעת מהן באמצעות איזון בין הענישה למניעה. יש הטוענים שההרתעה המותאמת הזו תתבסס על ארבע גורמים עיקריים, כדלהלן:¹⁰⁵

- הטלת סנקציות מדינתיות ואזרחיות¹⁰⁶ על פעולות תוקפניות במרחב הסב"ר.

¹⁰⁰ לדוגמה – על ידי חיוב חברות לחשוף פריצות שהתקיימו ברשתותיהן ועל ידי כך לחשוף אותן ללחצים של ציבור הלקוחות והמשקיעים.
¹⁰¹ Cyber Resilience – היכולת של רשת להמשיך ולפעול למרות תקיפות הנערכות כנגדה ו\או תאונות או תקריות בלתי מכוונות אחרות.

¹⁰² Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 13

¹⁰³ Will Goodman, *Op. cit.*, p. 106

¹⁰⁴ Liam Nevill, Zoe Hawkins, *Op. cit.*, pp. 15-1, 19

¹⁰⁵ Franklin D. Kramer and Aelanie J. Teplinsky, *Cybersecurity and Tailored Deterrence*, Atlantic Council, Dec. 2013, p. 2

¹⁰⁶ כולל מתן אפשרות וסיוע לגופים אזרחיים לתבוע את תוקפיהם על הנזק שנגרם להם.

- מתן הרשאה למספר מוגבל של שחקנים פרטיים לנהל הגנה פעילה במרחב הסב"ר בשיתוף פעולה עם הממשל. ההגנה הפעילה תתרכז בניסיון לאתר את התוקפים במרחב הסב"ר במידת ודאות גבוהה ותתרכז, לפחות בהתחלה, בהגנה על הבסיס התעשייתי הביטחוני.
- צמצום נקודות התורפה בתשתיות החיוניות – בעיקר במגזרי האנרגיה והפיננסים. זאת על ידי הנהגת אמות מידה מחייבות ומובחנות. הנהגת אמות המידה המחייבות תביא הן להגדלת הקושי לפגוע בתשתיות אלה והן לשיפור באיתנות התשתיות החיוניות שתתבטא בצמצום הנזק שיגרם מתקיפות במרחב הסב"ר.
- יצירת נורמות והסכמות בקרב מדינות שונות בנוגע לתקיפות במרחב הסב"ר ולתגובה אליהן.

הגבלת היקף ההרתעה

מודל ההרתעה הקלאסי (או הגרעיני) עוסק בהרתעה מפני עימותים. עם זאת, במרחב הסב"ר העימות כבר קיים והוא כנראה בלתי נגמר. בשונה מההרתעה הגרעינית, ההרתעה בסב"ר נדרשת כדי לעצב את מהלכו של העימות – להרתיע מפני צעדים ספציפיים (כגון תקיפת מטרות מסוימות או מסוג מסוים) או מפני שימוש בכלים ספציפיים, להרתיע מפני ניסיון להשיג יעדים מסוימים באמצעות מרחב הסב"ר (לדוגמה – התערבות בבחירות) וכו'. הרתעה זו היא דינמית יותר מאשר ההרתעה הגרעינית הקלאסית ונסמכת הן על איומים והן על פעולות – כולל נכונות להסלים את המצב לשם השגת הרתעה. הרתעה זו היא גם תגובתית וגם מניעתית. היא אינה מניחה ליריב ליטול את היוזמה ולכן לא יכולה להסתמך על הגנה ואיתנות בלבד. הרתעה זו אינה מתקיימת אך ורק באמצעות מרחב הסב"ר, אלא כוללת גם איומים ופעולות במרחבים אחרים כדי לקיים ולתחזק את ההרתעה בסב"ר. הרתעה זו, מטבעה, אינה מושלמת ואינה מתמדת, אלא היא בהכרח תופר, תשוקם ותשתנה עם הזמן.¹⁰⁷

הדיון על תקיפות במרחב הסב"ר נוטה פעמים רבות להיסחף לדיון בתרחישי קיצון, שמושויים לתקיפה גרעינית (או תקיפה מוסכמת רחבת היקף – כדוגמת המושג "פרל הארבור בסב"ר"). תרחישים קיצון כגון אלה נדרשים למענה קיצוני – כגון התערבות משמעותית של הממשלה, פיתוחים טכנולוגיים משמעותיים ונקיטה בקווי מדיניות מסוימים לצורך הרתעה ותגובה. עם זאת, רוב התקיפות במרחב הסב"ר אינן מקרי קיצון, אלא תקיפות קטנות, המתרחשות כדרך קבע. ההרתעה של תקיפות אלה (כמו גם של מעשי עוינות שאינם תקיפות) שונה באופן מהותי

¹⁰⁷ Eric Sterner, "Retaliatory Deterrence in Cyberspace", *Strategic Studies Quarterly*, Spring 2011, p. 69

מההרתעה הנדרשת כנגד מקרי קיצון.¹⁰⁸ אפשר שהרתעה שכזו תהיה אזרחית יותר, גמישה יותר וכלכלית יותר באופייה. כמו כן, אפשר ששיפור ההרתעה כנגד מקרי שגרה, אף שיהיה חלקי, יושג באמצעות שיפור זה או אחר בתנאים הקיימים ובמגבלות המערכת הקיימת. מנגד, אפשר גם שההרתעה במרחב הסב"ר ובאמצעות מרחב הסב"ר אכן קיימת רק כנגד מקרי קיצון כגון מעשים שיגרמו נזק פיזי, או אף נזק פיזי כבד.¹⁰⁹ במקרה כזה, אפשר שהמעבר לתגובה מידתית, או אף תגובה במרחב הפיזי, יהיה קל יותר. במידה מסוימת, דומה הרתעה זו להרתעה הגרעינית בכך שהיא מרתיעה מפני מקרי הקיצון, אך לא מרתיעה מפני פעולות אחרות הנמצאות מתחת לסף מקרי קיצון אלה (כגון, מלחמה בפריפריה, מלחמת פרוקסי וכו.). בהתאם, מעשים שאינם נחשבים פעולה לחימתית, כגון ריגול, מהווים סוגיה נפרדת להרתעה מאשר תקיפות במרחב הסב"ר (כדוגמת מניעת שירות או השחתת מידע וכו.). לכן, השיטות והאמצעים להרתיע פעולות "מתחת לסף התגובה" במרחב הסב"ר יהיו אחרים מאשר אלה שישמשו להרתעה מפני תקיפות במרחב זה.¹¹⁰

שילוב בין מרחב הסב"ר למרחב הפיזי

יש הטוענים שההרתעה במרחב הסב"ר היא עניין פשוט יותר להשגה בפועל מאשר מה שנתפס בתאוריה, בדיוק משום שמרחב הסב"ר אינו ניתן להפרדה מהמרחב הפיזי. לפי תפיסה זו, ההפרדה המלאכותית שאנו מקיימים רק מקשה עלינו להשיג את ההרתעה. משמע, עלינו לאמץ את סיכויי הזליגה של עימות ממרחב הסב"ר למרחב הפיזי ולפיכך לקיים יכולות מוסכמיות במרחב הפיזי, כחלק מהרתעה במרחב הסב"ר וההפך,¹¹¹ חיבור בין היכולות בסב"ר ליכולות במרחבים הפיזיים עשוי ללבוש כמה צורות, כגון יצירת מצב בו קיימות יכולות לתקיפה בסב"ר שלהן תוצאים במרחבים הפיזיים או אשר מסייעות באופן ישיר להשגת תוצאים שכאלה, ופיתוח יכולות סב"ר ההתקפיות שסייעו ליכולות הצבאיות המוסכמיות. אלה עשויים לשפר את ההרתעה בסב"ר על ידי יצירת היכולת להגיב על מעשים במרחב אחד באמצעות מרחבים אחרים וכמו כן, עשויות לשפר את ההרתעה של המדינה באופן כללי על ידי חיזוק עוצמתה הצבאית. עם זאת, המעבר בין המרחב הפיזי למרחב הסב"ר הוא דו-סיטרי וכך, מצב בו יכולותיה הצבאיות של המדינה חשופות לפגיעה משמעותית דרך מרחב הסב"ר עשוי לחבל בהרתעה הצבאית המוסכמית שלה בכל המרחבים. לבסוף, "העברת המלחמה

¹⁰⁸ Tyler Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options", in: Committee on Deterring Cyberattacks, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, Washington, DC: National Research Council, 2010, pp. 3-4

¹⁰⁹ Susan Hennessey, *Op. cit.*,

¹¹⁰ Will Goodman, *Op. cit.*, p. 124

¹¹¹ Will Goodman, *Op. cit.*, p. 109

למרחבים האחרים" עשוי לחזק את ההרתעה בסב"ר גם על ידי יצירת יכולת להימנע מ"מלחמת התשה בסב"ר" – עימות חשאי בעיקרו, שתוצאותיו עשויים להיות הרסניים (לפחות במרחב הסב"ר) מחד גיסא אך לא ברורים מאידך גיסא – ובמקום לערוך הרתעה בסב"ר באמצעות המרחבים הפיזיים.¹¹²

בהתאם, יש הטוענים שעליונות ההתקפה במרחב הסב"ר מחייבת אסטרטגיה של "תגובה בלתי מידתית" על התקפות במרחב זה. לפי תפיסה זו, כיוון שעליונות ההתקפה משותפת לכל הצדדים הפועלים במרחב הסב"ר, אמור להיווצר מצב של "שיתוק הדדי מובטח" שיביא להרתעה החדדית – בדומה להשמדה ההדדית המובטחת של הנשק הגרעיני. הרתעה זו לא תידרש ליכולת של ייחוס מדויק של תקיפה למקור, כיוון שהיא תסתמך על תפיסה לפיה גם ייחוס באופן שאינו ודאי מספיק לשם תקיפה. כמו כן, תסתמך תפיסה זו על הכרזה פומבית בדבר השימוש ב"שיתוק הדדי מובטח" כתפיסת הפעלה במרחב הסב"ר.¹¹³ עם זאת, גישה זאת אינה נותנת את הדעת על מידת הפגיעות השונה של מדינות שונות במרחב הסב"ר ועל קיומם של שחקנים שאינם חשופים להרתעה זו, כיוון שאינם נושאים באחריות לאוכלוסייה או לתשתיות, כגון שחקנים שאינם מדינתיים. כמו כן, לא נותנת גישה זו את הדעת על הקושי להצדיק תקיפה בלתי מידתית כנגד גורם שאפשר שאינו מעורב ולכן לא באמת נותנת מענה לאתגר הייחוס. לבסוף, גישה זו אינה נותנת את הדעת לסיכויים הסלמה או לגלישה אל מחוץ למרחב הסב"ר שעשויה להתרחש כתוצאה מתגובה בלתי מידתית, שעדיין תשאיר את היריב מסוגל לפעול הן במרחב הסב"ר והן מחוצה לו. תהליך ההסלמה הבלתי נשלט או נזק עצום וודאי יכולים לשמש להרתעה, כאשר ההסלמה מביאה לתוצאים קטסטרופליים – כגון מלחמה גרעינית. אך אין וודאות שאפשר להשיג זאת באמצעות מרחב הסב"ר, או לחילופין, שרצוי להשתמש באיום שכזה לשם הרתעה.

ניצול העמימות

החשאיות הרבה הכרוכה במרחב הסב"ר מציבה, כפי שאפשר לראות, אתגר משמעותי בפני ההרתעה.

יש הטוענים, שעמימות זו אינה אתגר, כי אם יתרון. זאת מכיוון, אפשר לטעון שהעמימות בנוגע לתוצאות האפשריות של מלחמה רבתי במרחב הסב"ר שמרה על מידה מסוימת של הרתעה עד כה.¹¹⁴ יש הטוענים אף שכדי להשיג יכולת הרתעה במרחב הסב"ר, לא נדרשת בהכרח

¹¹² Liam Neveill, Zoe Hawkins, *Special Report: Deterrence in Cyberspace – Different Domain, Different Rules*, Berton Australia: Australia Strategic Policy Institute, July 2016, p. 19

¹¹³ Matthew D. Crosston, "World Gone Cyber MAD – How Mutually Assured Debilitation Is the Best Hope for Cyber Deterrence", *Strategic Studies Quarterly*, Spring 2011, p. 103, 111

¹¹⁴ Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy", *Strategic Studies Quarterly*, Winter 2012, p. 109

הדגמה חיה ובאופן שאינו משתמע לשני פנים של יכולות במרחב הסב"ר – כמו שמושגת על ידי ניסוי ראש נפץ גרעיני - ומדינה יכולה להשיג הרתעה במרחב הסב"ר דווקא על ידי שמירה על "עמימות סב"ר". זאת כיוון שהרתעה עשויה לנבוע לא רק מחומרת העונש, אלא גם (ואולי בעיקר) מעצם הידיעה על העונש ומהסיכויים להיתפס ולהיענש. כך, תחושת פגיעות לכשעצמה – אמיתית או מדומיינת - עשויה לגרום להרתעה. דומה הדבר להרתעה הנגרמת על ידי ארגוני טרור. במקרים אלה, ההרתעה המבססת על תחושות איום ו"חדירות", המתבססת על יכולת חוזרת ונשנית של ארגון הטרור לבצע פיגועים – גם אם קטנים בהיקפם. פעילותם של ארגוני טרור נוטה להיות מלווה בפעילות הסברה ותעמולה פוליטיות המבהירות את הסיבה לפיגועים, מאדירה את יכולת הביצוע של הארגון ומבהירה את מטרותיו – גם ללא חשיפת השיטות והמקורות של ארגון הטרור.¹¹⁵ הפעולות הן פומביות ואילו ההרתעה מתבססת על היכולת לחזות את המעשים שיביאו את ארגון הטרור לתקוף ועל ההכרה ביכולתו של הארגון לממש את אימויו באופן מוצלח וסדיר.

אם נציב מנגד את ההרתעה הגרעינית, נראה שהיא הדגישה דווקא את חומרת התגובה (עד כדי השמדה הדדית וודאית) ואת המיידיות שלה (עקב הסיכוי לחסל את היריב לגמרי במכה אחת). אך הרתעה במרחב הסב"ר אינה חמורה כמו הרתעה גרעינית ואינה בהכרח מיידית, כיוון שקשה יותר לשתק לגמרי את היריב לטווח זמן ארוך (או לנצח) במכה אחת באמצעות מרחב הסב"ר, אלא היא מצריכה הדגשה של הוודאות, עקב האופי החשאי יותר של הפעילות במרחב זה. את העמימות במרחב הסב"ר אפשר להשיג על ידי פיתוח יכולת כל שהיא במרחב זה, שימוש בכלי תודעה כדי למצב יכולת זו כמשמעותית ואף ייחוס – מוצדק או לא - ברמז של מבצעים במרחב הסב"ר שיצביע על מוכנות של המדינה להשתמש במרחב וביכולות שבנתה, תוך שמירה על יכולת הכחשה של קשר ישיר למבצעים אלה. כיוון שבמרחב הסב"ר יכולת אחת יכולה לגרום למספר תוצאים, על שיח ה"הרתעה העמומה" להתמקד בתוצאים ובנכונות להפעילם ולא בהכרח ביכולות. מכאן שעל מדינות שמבקשות להשיג מידה זו או אחרת של הרתעה במרחב הסב"ר להיות ברורות בנוגע לתגובתן הצפויה במקרה של תקיפות כנגדן דרך מרחב הסב"ר ולא דווקא בנוגע ליכולות הספציפיות שהן מבקשות להפעיל.¹¹⁶ עמימות זו עשויה להשיג הרתעה דווקא עקב חוסר ההבנה של מרחב הסב"ר ושל היכולות הכרוכות בפעולה בו במרחב הציבורי ובקרב מקבלי ההחלטות. יש האומרים שסוג זה של מדיניות מופעל על ידי סין¹¹⁷ ובמידה מסוימת על ידי רוסיה.

עם זאת, קשה לחזות עד מתי תחזיק ההרתעה העמומה, בהינתן שחיקה הדרגתית עקב מעבר הזמן וההתרגלות לקיומו של מרחב הסב"ר מחד גיסא ובהינתן המשך בניין יכולות הסב"ר

¹¹⁵ Lawrence Freedman, *Op. cit.*, pp. 64, 122

¹¹⁶ Will Goodman, *Op. cit.*, pp. 105, 116

¹¹⁷ Matthew Crosston, *Op. cit.*, p. 108

שעשוי לגרות את מקבלי ההחלטות לעשות בהן שימוש, מאידך גיסא. אפשר אף שכבר כעת, הפעולות של רוסיה כנגד מערכת הבחירות האמריקנית בשנת 2016 מצביעות על שחיקה הולכת וגוברת של העמימות כגורם הרתעה במרחב זה. כך, ארה"ב מקיימת עמימות בנוגע ליכולותיה במרחב הסב"ר, אך התפיסה המקובלת היא שבידיה עוצמה בלתי מבוטלת במרחב הסב"ר. תפיסה זו נתמכת הן על ידי הדלפותיו של אדוארד סנאודן והן על ידי ייחוס התקפות שונות לארה"ב (כדוגמת Stuxnet). אף על פי כן, לא היה בכך די כדי למנוע התקפות סב"ר כנגדה על ידי רוסיה וסין, אפילו כנגד תשתיות ואינטרסים המוגדרים חיוניים, כדוגמת ההתערבות הגלויה למדי של רוסיה במערכת הבחירות האמריקנית.¹¹⁸ זאת מכיוון שכדי ליצור הרתעה (או אכיפה) באמצעות נשק כל שהוא, על האמצעי להיות מפחיד דיו כדי לגרום ליריב לשנות את התנהגותו או להימנע מהתנהגות מסוימת. ההרתעה אומנם יכולה לנבוע מאמונה כל שהיא, שאפשר שאינה מבוססת על המציאות. אך עם זאת, אם במשך זמן מסוים מודגם שימוש במרחב הסב"ר שאינו מביא לתוצאים משמעותיים, או מודגם חוסר נכונות (או יכולת) לחולל תוצאים מסוימים באמצעות המרחב, הרי שיש בכך כדי לשחוק את ההרתעה כולה.¹¹⁹ מכאן, אפשר אולי להניח שהרתעה אמיתית במרחב הסב"ר תהיה אפשרית רק לאחר "תצוגת תכלית" נרחבת של תוצאי פעולה צבאית גדולה במרחב הסב"ר (ואולי אף לא אז). לכן, אפשר שבסופו של דבר יהיה על הפעולה ההרתעתית בסב"ר להיראות ולא יהיה מנוס מהפגה מסוימת – אם כי, לא מוחלטת – של עננת העמימות הרובצת מעל הפעילות הצבאית במרחב הסב"ר לשם השגת הרתעה.¹²⁰

יצירת נורמות חדשות

כדי להשיג הרתעה במרחב הסב"ר, אפשר שידרשו כלים חדשים ושיטות חדשות, שילוו בנורמות חדשות. יש הטוענים שיצירת נורמות עשויה להיות תחליף מסוים (ומוגבל) להרתעה, כיוון שהיא תגביל הן את המטרות הנתקפות והן את חומרת התקיפות. מדובר בתוצאה השקולה להרתעה ספציפית, שתסתמך גם על אינטרס הדדי להימנע מתקיפות סב"ר, כנגד מטרות מסוימות.¹²¹

כיוון שמרחב הסב"ר הוא מרחב חדש, עם מאפיינים וחוקים ייחודיים, קשה, לעיתים, להשתמש בו בחלק מהנורמות והכלים הקיימים. לדוגמה, כלי הדין הפלילי העומדים לרשותנו כיום אינם מתאימים להרתעה מפני מעשים עוינים בסב"ר, כיוון שהם מחייבים עמידה בדיני ראיות והבאת

¹¹⁸ Benjamin Runkle, "The Best Strategy for Cyber-Conflict May Not Be a Cyber-Strategy", *War on the Rocks*, 08 Nov. 2016,

www.warontherocks.com/2016/11/the-best-strategy-for-cyber-conflict-may-not-be-a-cyber-strategy/

¹¹⁹ Matthew Crosston, *Op. cit.*, pp. 116-117

¹²⁰ Will Goodman *Op. cit.*, p. 108

¹²¹ P. W. Singer, *Op. cit.*,

העברייין לדין והשימוש בהם מצריך משך זמן ארוך (לעיתים ארוך מאוד – הן לחקירה והן להעמדה לדין). מאפיינים אלה מקשים על גורמי אכיפת החוק להתמודד גם עם שחקנים פליליים "רגילים" הפועלים בתוך המדינה, לא כל שכן עם שחקנים מדינתיים, שחקנים הנתמכים על ידי מדינה או שחקנים אחרים הפועלים מחוץ לגבולות המדינה דרך מרחב הסב"ר ואינם כפופים לחוקי המדינה. מנגד, שיקולים של נזק אגבי, חשש מהסלמה ומידתיות מקשים על שימוש בכלים צבאיים קינטיים לשם הרתעה במרחב הסב"ר. שימוש בכלים שכאלה נגד תקיפות סב"ר יחייב שינוי פרדיגמטי ונורמטיבי כך שפעולות עוינות במרחב הסב"ר יתפסו כשקולות לפעולות עוינות במרחב הפיזי, גם אם הן לא הביאו לנפגעים בנפש, אלא רק לנזק כספי. שינוי פרדיגמטי נוסף הוא זניחת הצורך למצוא את התוקף הספציפי במידת ודאות גדולה והסתפקות במידות וודאות נמוכות יותר ו\או בזהות כללית יותר של התוקף (במקום אדם ספציפי, ארגון או אף מדינה האחראים לתקיפה) לשם פעולה נגדו. עוד שינוי שעשוי להידרש נוגע להטלת אחריות על "צד שלישי" שמעורב בתקיפות – בין אם בהסכמה ובין אם שלא בהסכמה – החל מחברות המחזיקות שרתים המשמשים את התוקפים וכלה במדינות שנראה שהתקיפה יצאה משטחן. פעולה מהירה יותר נגד תקיפות סב"ר עשוי לחייב הורדת סמכות הביצוע לדרגים נמוכים יותר וניסוח "נהלי העסקה" (Rules of Engagement) למרחב הסב"ר, שיאפשרו גם למקבלי החלטות זוטרים יותר לפעול במרחב זה ודרכו, ללא צורך להגיע עד למקבלי ההחלטות ברמה הלאומית. צעדים אלה נכונים גם במידה ומבקשים להגיב על תקיפות במרחב הסב"ר בכלים שאינם קינטיים – כגון מבצעי גמול במרחב הסב"ר או כלים דיפלומטיים כגון סנקציות. יש אף הטוענים כי נדרשים גם מגוון צעדי הרגעה (Reassurance) במרחב הסב"ר כגון הכרזה פומבית בדבר מעשים במרחב הסב"ר שהמדינה תימנע מהם – כמו פגיעה בכורים גרעיניים פעילים או בתשתיות חיוניות בכלל. צעדים שכאלה אולי אינם יעילים באכיפת הרתעה, אך הם נחשבים לתנאי מחזק הרתעה.¹²² השינויים הנורמטיביים יחייבו גם מגוון פיתוחי משנה בתחומים שונים, החל מהערכת השפעות מסדר שני ושלישי לתקיפות סב"ר, דרך פיתוח שיטות וכלים לזיהוי תקיפות ומקורותיהן וכלה בכלים, תוכניות וחוקים שיאפשרו תגובות מדודות ומוגבלות. שינויי המדיניות שינהגו בנוגע למרחב הסב"ר ידרשו להיות פומביים (ואפשר שידרשו להדגמה חיה או אף למספר הדגמות חיות) כדי להרתיע ולמנוע אי הבנות. עם זאת, הם לא ידרשו להיות מפורטים מידי ואף ידרשו להשאיר בידי המדינה מרחב תמרון ניכר יחסית – במיוחד בעת קביעת התקדימים.¹²³

¹²² Will Goodman, *Op. cit.*, pp. 105, 109

¹²³ Eric Sterner, "Retaliatory Deterrence in Cyberspace", *Strategic Studies Quarterly*, Spring 2011, p. 71-74

סיכום ומסקנות

סוגיית ההרתעה היא מהמורכבות הקיימות בשדה היחסים הבין לאומיים. מרחב הסב"ר מוסיף על מורכבות זו הן עקב טבעו והן עקב החידוש בו. לפיכך, קשה מאוד לסכם את הנושא באופן דפיניטיבי ורבות עוד יכתב בו. עם זאת, אפשר להעלות מספר נקודות שיש לתת עליהם את הדעת.

ראשית, קיים פער ביכולת ההרתעה על ידי ענישה. זאת כיוון שכיום, במרחב הסב"ר תוקפים מסוגלים לשמור על אלמוניותם במידה משמעותית, דבר המצמצם מאוד את הסיכוי לאתרם ולהעמידם לדין. כמו כן, תוקפים הפועלים מטעם מדינות – באופן ישיר או באופן עקיף – מסוגלים גם להתחמק מעונש. לא זו אף זו, פעמים רבות, המדינות (או הארגונים) המבצעות את מעשה התוקפנות במרחב הסב"ר מסוגלות גם הן להתחמק מעונש – בין אם באמצעות שמירה על ספק סביר באשר למעורבותן ובין אם עקב הרתיעה של הנתקף מלהגיב באופן חמור דיו. לבסוף, גם בהנחה שהתוקף ושולחו מאותרים במידת ודאות מספקת, עדיין נשאלת השאלה האם פגיעה במרחב הסב"ר שווה את ההסלמה (שעשויה להפוך בלתי נשלטת) במרחב הפיזי. אולם, בד בבד, במרחב הסב"ר הפגיעות היא כה גדולה והעליונות של התוקף כה ניכרת עד שקשה מאוד לחשוב על אסטרטגיה יעילה של הרתעה באמצעות מניעה. ההנחה היא שתמיד תימצא פרצה וסביר שהעלויות של מציאתה עשויים להיות מצומצמות יחסית לתועלת. עם זאת, אפשר להניח שעבור שחקנים חלשים ומעוטי אמצעים – כגון פושעים קטנים או אקטיביסטים לא מאורגנים – חיזוק הגנות הסב"ר עשוי לשמש כגורם מרתיע, גם אם לא יוכל להרתיע יריבים מדינתיים (או אף יריבים פליליים מאורגנים), שהוכיחו עצמם מסוגלים לפרוץ מערכות מאובטחות עד מאוד.

שנית, יש בעיה של "מודעות מצבית" ו-וודאות. הרתעה, באשר היא, מחייבת מידה מסוימת של ודאות – הן ודאות באשר לזהות התוקף והן ודאות באשר לאופי התגובה והשפעותיה או למידת הקושי להשיג את מטרות הפעולה מצד "המורתע". הודאות לא נדרשת להיות מלאה – הרי גם בהרתעה הגרעינית היה תמיד ספק שמא "ילחץ היריב על הכפתור האדום" – אך היא נדרשת להתקיים במידה גבוהה מספיק כדי לגרום לפעולה או להניא ממנה. במרחב הגרעיני, עמלה ארה"ב רבות כדי להשיג יכולת הרתעה. לדוגמה, היא פיתחה יכולות לאתר מהיכן הגיעו החומרים הבקיעים ששימשו לנשק גרעיני מסוים, היא פיתחה יכולות גלויות להפעיל נשק גרעיני על מטרות בכל רחבי העולם במידת ודאות גבוהה, גם לאחר שנפגעה בעצמה ממכה גרעינית ניכרת והיא פיתחה יכולות התראה כנגד התקפה גרעינית. עוד עמלה ארה"ב רבות על העברת מסר ברור מספיק באילו מקרים בכוונתה להשתמש בנשק גרעיני ובאילו לא וכיצד

בכוונתה להגיב על מקרים שונים של שימוש בנשק גרעיני, פיתוחו או הפצתו.¹²⁴ ולמרות כל זאת, גם בשיא המלחמה הקרה, כאשר תמונת היכולות ההדדית הייתה יחסית ברורה, התקיימו פערי ההבנה – לעיתים משמעותיים – בין הסובייטים לאמריקנים. אפשר רק להניח מה יקרה כאשר תמונה זו לא תהיה ברורה, עקב החשאיות המובנית של פעולה במרחב הסב"ר.

הודאות היחסית שהייתה קיימת בימי המלחמה הקרה – על כל הערכות המודיעין החסרות והשגויות משני הצדדים – חסרה מאוד במרחב הסב"ר. מרחב הסב"ר חדש מידי ו"עכור" מידי. לאף אחד לא ברור איך תיראה תגובה במרחב הסב"ר, מה יכולות להיות השפעותיה, מה הסיכוי לענישה – במרחב הסב"ר או במרחב הפיזי – בתגובה על תוקפנות במרחב הסב"ר, כיצד לייחס תוקפנות לתוקף במידת ודאות מספקת ואפילו מה הן הפעולות שעשויות לגרום בעקבותיהן תגובה. האופי החשאי והבלתי מובן של מרחב הסב"ר והיעדר הקונצנזוס בנוגע לשימושים הצבאיים בו וללגיטימיות שלהם, עשוי להקשות, בעת זו, על היכולת להסביר את מדיניות ההרתעה בסב"ר הן לדעת הקהל הפנימית, הן לזו הבין לאומית ועל אחת כמה וכמה, ליריב. מכאן שאפשר שלא תושג מידת הודאות המינימלית הנדרשת לשם הרתעה.

אתגר שיוך התקיפה לתוקף אף הוחמר באחרונה עם החתירה תחת אמינות סוכנויות המודיעין אותה אפשר היה לראות בחודשים נובמבר 2016 – ינואר 2017 בכל הנוגע לאירועי ניסיונות ההשפעה של רוסיה על מערכת הבחירות האמריקנית. כך, אפשר שבעתיד יצליחו סוכנויות המודיעין לאתר את התוקף במידת אמינות גבוהה יחסית, אך שדעת הקהל לא תאמין להן כלל – הן עקב חוסר אמון כללי בסוכנויות המודיעין והן עקב התפיסה שאומרת שמודיעין סב"ר הוא כה רגיש, עד שהממשל לעולם לא ישחרר מודיעין אמיתי ורגיש לציבור, גם על מנת להצדיק את מעשיו. את הבעיה שבצורך לחשוף מקורות לשם תגובה יעילה במרחב הסב"ר אפשר היה לראות גם בחודשים האחרונים, בדו"חות שפרסמה הבולשת הפדרלית האמריקנית¹²⁵, כהצדקה לייחוס הרוסים לניסיונות ההשפעה על מערכת הבחירות האמריקנית. דו"ח זה, שהיה בלתי מסווג, היה מבולגן וחסר מאוד בפרטים ואפשר שפגע בניסיונות התגובה של ארה"ב, בהצדקה שלהן ובתוך כך, גם ביכולת ההרתעה האמריקנית.¹²⁶ אכן, אפשר לראות שמומחי

¹²⁴ Clorinda Trujillo, *Op. cit.*, p. 45

¹²⁵ הממשל האמריקני פרסם שני דו"חות על ההשפעה הרוסית על הבחירות בשנת 2016. הראשון – שהיה ממוקד יותר בפריצה של גורמים רוסיים לרשתות המפלגה הדמוקרטית: *Grizzly Steppe – Russian Malicious Cyber Activity*, JAR-16-20296A, 29 Dec. 2016, www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf;

השני – שהיה כללי יותר ועסק בניסיונות ההשפעה של רוסיה על הבחירות לא רק באמצעות הסב"ר: *Assessing Russian Activities and Intentions in Recent US Elections*, ICA 2017-01D, Washington, DC: Office of the Director of National Intelligence, 06 Jan. 2017, www.dni.gov/files/documents/ICA_2017_01.pdf

¹²⁶ Dan Goodin, "White House Fails to Make Case That Russian Hackers Tampered With Elections", *Ars Technica*, 31 Dec. 2016, www.arstechnica.com/security/2016/12/did-russia-tamper-with-the-2016-election-bitter-debate-likel

אבטחה אזרחיים רבים אינם מאמינים לייחוס תקיפה קודמים שקבע הממשל האמריקני, כגון בקשר לזהות התוקפים בפריצה לחברת סוני בשנת 2014.¹²⁷ מכאן אולי אפשר להבין מדוע, לפי דעתם של מספר מומחי אבטחה אזרחיים, בוחרים האקרים רוסים, מאז 2014, שלא להשקיע מאמץ רב בהסתרת זהותם.¹²⁸ עובדה זו משמעה שלתפיסתם, ההרתעה בסב"ר מוגבלת מאוד.

נראה שבכל מקרה, הגדלת העמימות ואי הוודאות במרחב הסב"ר אינה משרתת את מטרות ההרתעה. לפיכך, יצירת הרתעה עשויה לחייב החלטה ברורה לצמצם במידה ניכרת את העמימות, למרות המחירים הכרוכים בכך. אפשר שמחירים אלה גבוהים מידי ביחס לתועלת הנובעת מההרתעה בסב"ר. אפשר, שבדומה להרתעה הגרעינית, ידרשו שנים רבות ומגוון פיתוחים טכנולוגיים כדי לייצב ההרתעה במרחב הסב"ר. אפשר אף שיידרש לשם כך "אירוע מכונן", בו תופעל יכולת סב"ר באופן ברור ורחב היקף, שיחרוט בזיכרון הקיבוצי כיצד נראית תגובה גלויה, קיצונית ואלימה בסב"ר.¹²⁹

כך או כך, יש לדון בבירור בסוגיה בדרגים של מקבלי ההחלטות ולהימנע מאמירות כלליות¹³⁰ או מאמירות חסרות כיסוי¹³¹, הנוטות לעיתים ללוות את תחום הסב"ר באופן כללי ואת ההרתעה בפרט.

כמו כן, עלינו גם לתת את הדעת לנורמות ההולכות ומתגבשות כיום. מערכת הבחירות האחרונה בארה"ב והשימוש העוין שנעשה במרחב הסב"ר כנגד ארה"ב על ידי רוסיה במהלכה מעלים שוב לכותרות את סוגיית ההתערבה במרחב הסב"ר. באופן כללי, מאז מתקפת הסב"ר על אסטוניה בשנת 2007 ועד תקיפות משמעותיות כנגד תשתיות חיוניות¹³², ופריצות לצרכי מודיעין למוסדות ממשל¹³³ ולתעשיות ביטחוניות¹³⁴, בחרו ממשלות שלא להגיב באופן עצים או גלוי, קינטי או שלא קינטי, על מעשי עוינות במרחב הסב"ר. כך, התגובה ("לפי פרסומים זרים")

[y-to-rage-on](#); Lorenzo Franceschi-Bicchierai, "The Declassified Report on Russia's Election Hacking Says Nothing New", *Motherboard*, 7 Jan. 2017,

www.motherboard.vice.com/en-us/article/the-declassified-report-on-russias-election-hacking-says-no-thing-new

¹²⁷ Brian Krebs, "The Download on the DNC Hack", *Krebs On Security*, 03 Jan. 2017,

www.krebsonsecurity.com/2017/01/the-download-on-the-dnc-hack

¹²⁸ Kelly Jeckson Higgins, "Mandiac: Russian State Hackers Changed the Game", *Dark Reading*, 01 Dec. 2016,

www.darkreading.com/threat-intelligence/mandiac-russian-state-hackers-changed-the-game-/d/d-id/1327616

¹²⁹ יש לציין שאירוע מכונן עשוי דווקא לסכל את יכולת ההרתעה בסב"ר. אם תוצאות האירוע המכונן לא יהיו קשות מספיק, אפשר שהאירוע ייצור דימוי שפעולות במרחב הסב"ר הן דבר מה שאפשר – או אף קל – להתמודד עימו. במובן זה, אפשר שהתקיפות היום-יומיות המתנהלות במרחב הסב"ר מסכלות כל העת את היכולת להשיג הרתעה במרחב זה.

¹³⁰ כגון "יש להרתיע את האויב בסב"ר".

¹³¹ כגון "תקיפת סב"ר על ידי מדינה זרה עשויה להיחשב למעשה לוחמתי ועשויה לגרום תגובה מוחצת".

¹³² כגון הפלת שלוש תחנות כוח באוקראינה בדצמבר 2015

¹³³ כגון הפריצה למחשבי סוכנות כוח האדם של הממשל האמריקני (OPM) שהתגלתה ביוני 2015

¹³⁴ כגון הפריצה למחשבי לוקהיד מרטין שהתגלתה במאי 2011

של ארה"ב לתקיפה כנגד חברת סוני, המיוחסת לצפון קוריאה, נערכה במרחב הסב"ר וללא ייחוס לארה"ב עצמה. מכאן עשויה לצמוח הנורמה לפיה על התקפות במרחב הסב"ר – גם כנגד גורמים מסחריים – מגיבים במרחב הסב"ר. מנגד, סנקציות כלכליות ומשפטיות שהושטו כנגד אנשי צבא סינים החשודים בתקיפות סב"ר נגד ארה"ב עשוי להביא ליצירת נורמה של שימוש בכלים אחרים – דיפלומטיים ומשפטיים – כתגובה על התקפות במרחב הסב"ר. לבסוף, אכן ישנן דוגמאות לתקיפות פיזיות כנגד גורמי טרור הפועלים במרחב הסב"ר¹³⁵, אך עדיין לא ברור האם ההצדקה לתקיפות אלה היא החברות בארגון טרור או התקיפות במרחב הסב"ר.

אפשר לראות שבכל המקרים שתוארו לעיל, גם כאשר נערכה תגובה גלויה, היא התבטאה יותר בכלים דיפלומטיים (כגון סנקציות) או משפטיים ובכל מקרה הייתה פחות חמורה מהתקיפה. אירועים אלה, כמו גם חשיפת פעולות הריגול של ארה"ב אחרי מדינות רבות באמצעות מרחב הסב"ר ופרשיות אחרות כגון Suxtnet מביאים בהדרגה את מערכת הנורמות ואת דעת הקהל לאימוץ תפיסה של היעדר תגובה גלויה על התקפות במרחב הסב"ר וניתוק בין פעולות במרחב הסב"ר לפעולות (גלויות) במרחב הפיזי. כמו כן, מערכת הנורמות המתהווה מציבה סף גבוה מאוד בכל הנוגע לייחוס התקיפה לתוקף וכרגע, נדרש ייחוס כמעט וודאי כדי להצדיק תגובה – בטח ובטח במרחב הפיזי. לפיכך, הנורמות המתגבשות כיום מסכלות באופן משמעותי את ההרתעה, למרות שממשלות מנסות כל העת להתבטא באופן תקיף ומאיים (אך מעורפל), על מנת להרתיע הישנות של מקרים אלה. אפשר להניח שההרתעה בסב"ר, כיום, מוגבלת מלכתחילה ומגמה זו מעלה סימן שאלה את היכולת לקיים הרתעה במרחב הסב"ר גם בעתיד. בהיעדר שינוי במגמות הקיימות, אפשר לשער שהנחת המוצא של תוקפים עתידיים כי התגובה האלימה והגלויה לתקיפות בסב"ר תהיה מוגבלת.

כל זאת מתווסף לבעיות השורש של תפיסת ההרתעה – חוסר היציבות המובנה שלה - כפי שאפשר לראות מדינמיקת ההרתעה הגרעינית במלחמה הקרה. אז, למרות קיומו של נשק שיכול, באופן כמעט מוכח, להביא לסוף הקיום האנושי ולמרות הבנה סובייטית כי אי אפשר יהיה לנצח מלחמה גרעינית, פיתחו שני הצדדים תפיסות הרתעיות שאפשרו קיום כל שהוא של מלחמה בין מעצמתית – שעשויה הייתה להביא למלחמה ש"אי אפשר לנצח בה". בהתחשב באופי הטוטאלי כל כך של ההרתעה הגרעינית ובעובדה שגם הוא נמתח לעיתים עד כדי סף הקריסה, נשאלת השאלה האם בכלל אפשר לקיים לאורך זמן הלך רוח של הרתעה כוללת – בסב"ר או מחוצה לו - ואם לא, האם לא עדיף לבנות מלכתחילה תפיסת הרתעה מוגבלת שתאפשר בצורה זו או אחרת השגת יעדים מדיניים באמצעות הפעלת כוח.

¹³⁵ Mark Hosenball, "British Hacker for Islamic State Killed in US Drone Strike in Syria: Sources", Reuters, www.reuters.com/article/us-mideast-crisis-hacker-isUSKCN0Qv2KA20150827

לכן, אפשר שאין זה מציאותי לנסות לקיים מדיניות הרתעה כוללנית בסב"ר ועשוי להידרש לסב"ר מודל הרתעה חלופי. במקום להביט על ההרתעה הגרעינית כמודל, אפשר שנדרשים אנו להביט על הניסיון להרתיע מעשי טרור כמודל להרתעה במרחב הסב"ר. המערכה כנגד הטרור נדרשת להתמודד עם מספר רב יותר של אויבים חמקנים יותר, שמעשיהם נערכים בחתימה נמוכה, שקשה לכייל את מידתיות התגובה נגדם ושלא תמיד ברורה מידת האחריות של השחקן המדינתי שבתוכו הם פועלים. בעוד שההרתעה הגרעינית הצליחה עד כה במשימתה למנוע הפעלה כל שהיא של נשק גרעיני, הצלחת ההרתעה נגד הטרור מוגבלת יותר וההרתעה כנגד הטרור אינה עניין מוחלט ו"בינארי".¹³⁶ כמו כן, יש להביא בחשבון שכיוון שגורמים שונים פגיעים במידה שונה במרחב הסב"ר, אפשר שלא יהיה כלל יעד מתאים לתגובה – ולפיכך גם להרתעה – במרחב הסב"ר.¹³⁷ בהתאם, עקב מורכבות מרחב הסב"ר, הערפל היחסי השורר בו ומגוון השחקנים הרב והמגוון הפועלים בו, אפשר שמשטרי הרתעה במרחב הסב"ר לא יתבססו על אסטרטגיית הרתעה אחת המתאימה לכל השחקנים באשר הם, אלא ידרשו גם הם להיות צרים וספציפיים – כנגד יריבים מסוימים, בהגנה על מערכות מסוימות או אינטרסים מסוימים ותוך שימוש באמצעים מסוימים, על מנת להרתיע מפני פעולות מסוימות.¹³⁸ ככל הנראה יידרשו אסטרטגיות שונות להרתעת שחקנים מדינתיים ולהרתעת שחקנים שאינם מדינתיים במרחב הסב"ר. סביר גם שכל שחקן יידרש לאסטרטגיית הרתעה מותאמת אישית, שתתחשב במאפייניו, בנקודות החוזק והתורפה שלו, כדי להרתיעו. סביר גם שאסטרטגיות הרתעה אלה לא יהיו כוללות, אלא ממוקדות בניסיון להרתיע מביצוע פעולות ספציפיות במרחב הסב"ר.

כך, אפשר שאסטרטגיית הרתעתית מסוימת תסתמך על מניעת הישגים מהיריב, על ענישה או אף על תגובה מחוץ למרחב הסב"ר – תלוי באופיו הייחודי של היריב ובמטרותיו. סביר שהרתעה של שחקנים שונים תצריך שימוש בכלים שונים – לדוגמה כלים פליליים כנגד גורמי פשיעה (גם אם הם בשליחות של שחקן מדינתי) וכלים צבאיים ודיפלומטיים כנגד מדינות. אפשר גם שיריבים מסוימים יהיו חשופים יותר למבצעי השפעה, בעוד שאחרים יהיו חשופים יותר לפגיעה באינטרסים כלכליים או לאיום על תשתיות חיוניות וכו'.¹³⁹ לכן, מכאן, אפשר שאין כלל אסטרטגיית הרתעה למרחב הסב"ר באופן כללי, אלא שהפעולה במרחב זה היא אך ורק כלי במסגרת האסטרטגיית הכוללת כנגד יריב זה או אחר ומושתתת הן על הרתעה והן על עקרונות אסטרטגיים אחרים, לפי הצורך.

¹³⁶ Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security*, Vol. 7 No. 1, 2014, p. 61-62

¹³⁷ Will Goodman, *Op. cit.*, p. 112

¹³⁸ Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 12

¹³⁹ Benjamin Runkle, *Op. cit.*,

אפשר שההרתעה בסב"ר תהיה אמינה רק כאשר התקיפה בסב"ר תהיה כלי אחד מבין מספר כלים מגוונים – כולל תקיפות קינטיות - ורק כאשר קיימות הן הנכונות והן היכולת להסלים אל מחוץ למרחב הסב"ר (ולשאת בתוצאות).¹⁴⁰ כך, כדי ליצור הרתעה, נדרשת המדינה ליצור מנעד לפעולה ותגובה במרחב הסב"ר ובאמצעותו וכמו כן, נדרשת למידה מסוימת של עליונות בהסלמה (Escalation Dominance)¹⁴¹ כדי לנצל את מנעד הכלים שברשותה. באמצעות מנעד זה תוכל המדינה לשמור על גמישות באפשרויות התגובה שלה וכך ליצור את הרושם שהיא יכולה ונכונה להגיב במרחב הסב"ר ובאמצעותו, הן על פעולות פיזיות והן על פעילויות סב"ר כנגדה. במידה רבה, דומה הדבר להרתעה במרחב הפיזי. שם, עומד לרשות המדינה מנעד רחב של אפשרויות פעולה שונות, הכולל הן נכסים להרתעה מסדר גבוה, המרתיעים מפני פעולה בעצימות גבוהה (כגון כוחות צבאיים מאומנים ומצוידים) והן נכסים להרתעה מסדר נמוך, המרתיעים מפני ניסיונות להשיג יעדים באמצעים הדרגתיים ובעצימות נמוכה ("שיטת הסלאמי" – כגון כוחות שיטור כגון משמר חופים ומשמרי גבול ג'נדרמריות). נכסים אלה משלימים אחד את השני ומחזקים אחד את השפעתו של השני ואי אפשר להשיג מידה רבה של הרתעה או של ביטחון ללא שילוב ביניהם.¹⁴² לכן, אפשר שגם במרחב הסב"ר תידרש המדינה למצוא אמצעים ושיטות להרתיע מפני פעולות עצימות (כגון פגיעה בתשתיות לאומיות) ופעולות הדרגתיות (כגון ריגול, הדלפת מסמכים ו"הטרדות" אחרות בעצימות נמוכה) ושאמצעים אלה לא יוגבלו למרחב הסב"ר בלבד.

לבסוף, כיוון שמגוון השחקנים במרחב הסב"ר כה גדול, מידת הפרדה וההבחנה ביניהם נדרשת להיות משמעותית גם כן. לכך השלכות בכל הנוגע לאיסוף המודיעין ולשיתוף הפעולה הבין סוכנותי הכרוכים במאמצי ההרתעה. ככל דבר במרחב הסב"ר, סביר שגם ההרתעה תהיה מאמץ כלל מדינתי, שישתמש בשילוב של כל כלי העוצמה הלאומית ויצריך פעולה משולבת של מספר סוכנויות שונות, המגזר הפרטי ואף גורמים בין לאומיים שונים.

¹⁴⁰ Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 11

¹⁴¹ מצב בו לשחקן יכולת להסלים את העימות בדרכים שיהיו לרעת יריבו, בעוד שהיריב לא יוכל לעשות כן – בין אם כיוון שאין לו אפשרויות להסלים את העימות, או שהאפשרויות שעומדות לרשותו לא ישפרו את מצבו.

Forrest E. Morgan et. al., *Dangerous Thresholds – Managing Escalation in the 21st Century*, Santa Monica, CA: RAND, 2008, p. 15

¹⁴² Jonathan F. Solomon, *Op. cit.*, p. 145

נספח א' - קיצור תולדות ההרתעה (בעת המודרנית)

המלחמה הקרה מספקת דוגמה לאופן בו הבדלים תרבותיים ופערי אמון עשויים להביא לכך שמדיניות של הרתעה על ידי צד אחד תיתפס כמדיניות תוקפנית על ידי צד שני. בחינה קצרה של תפיסות ההרתעה במערב ובמזרח בימי המלחמה הקרה תאפשר להבין טוב יותר את המושג באופן כללי ואת נקודות החוזק והחולשה שבו.

ההרתעה במערב

השימושים הראשונים במושג ההרתעה החלו בשנות ה-20 וה-30 של המאה ה-20, בהקשרי הלוחמה האווירית. תפיסה זו טענה כי רק היכולת המוכחת לגרום להרס רב באמצעות כוח אווירי תוכל להניא את היריב מלהפעיל כוח אווירי בעצמו. תפיסה זו התגלתה כפשטנית מידי במלה"ע 2, בה הופעלו באופן נרחב כוחות אוויר למטרות הפצה אסטרטגית על ידי רוב הצדדים. אף על פי כן, הומרה התפיסה לאחר המלחמה ויושמה על הנשק הגרעיני. יש הטוענים שההרס המשמעותי שתגרום מלחמה גרעינית הצליח לשמש כמרתיע מפני מלחמה מעצמתית מאז.¹⁴³

רעיון ההרתעה הגרעינית החל להשתרש בשנות החמישים של המאה העשרים, ככל שגדלה העוצמה של כלי הנשק הגרעיניים ותפוצתם – ובהתאם החל להתברר שאין באמת דרך להילחם במלחמה גרעינית ללא הרס אדיר. הגל הראשון של תורת ההרתעה הגרעינית גרס כי אפשר להרתיע אויב ממלחמה קונבנציונלית על ידי איום בשימוש בנשק גרעיני. חלק מההרתעה שבמלחמה הגרעינית הייתה שגם מספר קטן יחסית של ראשי קרב גרעיניים יכולים לגרום לנזק עצום. לפיכך, גם הגנה טובה ככל שאפשר, עשויה שלא לספק את רמת ההגנה הנדרשת כדי להימנע מעלויות גבוהות ואף קטסטרופליות – מכאן, להתקפה עליונות משמעותית. בהדרגה חלה מתיחה של מושג ההרתעה והוא החל להיות מוכל גם על עימותים קטנים, פעולות עוינות מוגבלות (או הפעולות העוינות כולן) ופעולות עוינות שכבר החלו ונמצאות כעת בעיצומן. בהתאם, ההרתעה החלה ללוש מאפיינים של איום בהשמדה הדדית ובהפעלת כוח לא מידתית. בהדרגה, הפכה ההרתעה הגרעינית ל"כללית" – כלומר, למאפיין הקיים תמיד ברקע ההתנהלות הבין מעצמתית. ההרתעה הגרעינית השפיעה על תפיסת הפעלת הכוח הצבאי בכללותו. כיוון שהשגת הכרעה קונבנציונלית של היריב עשויה הייתה להביא להסלמה גרעינית, הפכה גם ההכרעה הקונבנציונלית למסוכנת. לכן, הכוח הצבאי הקונבנציונלי אמור היה לשפר את עמדת המיקוח כנגד היריב ולא בהכרח להכריעו. בהדרגה התפיסה שאפשר להרתיע מלחמה קונבנציונלית באמצעות איום בנשק גרעיני השתנתה והחל "הגל השני" של

¹⁴³ Lawrence Freedman, , pp. 9-10; Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 4

תורת ההרתעה. שינוי זה נבע הן מכיוון שהנשק הגרעיני השתכלל והתעצם והן כיוון שגם הסובייטים (ולאחר מכן גם הסינים) השיגו נשק גרעיני ולבסוף גם יכולת מכה שניה אמינה. במצב זה, התגבשה ההבנה שאי אפשר לנצח במלחמה גרעינית, כיוון שלעולם אי אפשר יהיה להבטיח נזק מספיק שימנע מהיריב להפעיל את יכולותיו הגרעיניות – ולגרום עקב כך נזק עצום (ואף סופני) לתוקף - ולכן אפשר רק לאיים בשימוש בנשק זה, אך לא בהכרח להשתמש בו. בהתאם לכך, נשאלה השאלה מה אמינותו של האיום הגרעיני, אם ברור שהוא יביא למלחמה שאף צד אינו יכול לנצח בה. בשנות ה-60 של המאה העשרים החלו במערב להשתמש במושג ההשמדה הוודאית ההדדית (Mutual Assured Destruction – MAD). מושג זה ביטא את הביטחון של שני הצדדים ביכולתם להשמיד אחד את האחר באמצעות נשק גרעיני. לפיכך, שני הצדדים הגיעו לשוויון ולהרתעה הדדית. במצב זה, הפתיחה המכוונת במלחמה נתפסה כלא הגיונית, אך עם זאת, עדיין נותרה האפשרות של הסלמה לא מכוונת ובלתי נשלטת. לפיכך, הפכה ההרתעה הגרעינית מכלי מידי למניעת מלחמה לכדי להבטחת היציבות ארוכת הטווח. לא ברור לגמרי כיצד ההרתעה הגרעינית החזיקה מעמד וחלקה במניעת מלחמה בין המעצמות נמצא במחלוקת בקרב החוקרים. אכן, היו מספר מקרים במהלך המלחמה הקרה בהם היא כמעט כשלה. כמו כן, יש לזכור שההרתעה הגרעינית אומנם מנעה מלחמה גרעינית כוללת בין המעצמות, אך לא מנעה את המלחמות הקטנות יותר בין מעצמות לצדדים שעבדו בשירות המעצמה השנייה.¹⁴⁴ אף על פי כן, ההרתעה הגרעינית שרדה גם כאשר הסובייטים השיגו נשק גרעיני ויכולת לתקוף באמצעותו את ארה"ב גופא. לעמידות ההרתעה באותן השנים ניתנו מספר הסברים כדלהלן:¹⁴⁵

- המדיניות הכוללת של ארה"ב הייתה מדיניות הכלה ולא מדיניות הרתעה – זאת כיוון שהבסת הגוש הקומוניסטי או פיוסו לא נראו כאפשרויות פעולה סבירות. מדיניות הכלה האמריקנית דגלה באיום בשימוש בכוח כדי לבלום את התפשטות הקומוניזם ובשימוש בכוח במקומות בהם התפשטותו נמשכת. ההרתעה הייתה כלי בשירות מדיניות הכלה.
- ההרתעה הגרעינית הייתה הדדית – כל שימוש בנשק גרעיני על ידי אחד הצדדים נראה כהתאבדות של שניהם. הארסנל ההולך וגדל של נשק גרעיני תמך בתפיסה זו. לפיכך, הפעלת נשק גרעיני נתפסה כצעד חסר הגיון אסטרטגי (ובעייתי מבחינה אתית) - על אף הצהרות תקיפות ותכופות של ממשלות המערב בדבר הנכונות להפעיל נשק גרעיני במקרה הצורך – הצהרות שהיה בהן צורך בדיוק משם שהפעלת נשק גרעיני נראתה כצעד משולל היגיון.

¹⁴⁴ Lawrence Freedman, *Op. cit.*, p. 11-14, 16, 37

¹⁴⁵ *Ibid*, p. 11-14

- ההרתעה התקיימה בסביבה יציבה יחסית, בה שני הצדדים (שהיו צדדים ברורים ודיכוטומיים, יחסית) היו מחויבים ל"מאבק ארוך" ולא בסביבה בה אחד הצדדים היה מעוניין בהכרעה מיידית של הצד האחר. הסביבה היציבה הזו הביאה להטמעת תפיסת ההרתעה הן בקרב מקבלי ההחלטות והן בקרב הקצונה. בהדרגה, כל פעולה שמטרתה לשמור על הסטטוס קוו הבין מעצמתי – ולכן כמעט כל הפעולות בזירה הבין מעצמתית – החלה להיחשב כהרתעה.

בשנות ה-70 של המאה ה-20 החל גל שלישי של תורת ההרתעה. גל זה הטיל ספק במידת הרציונליות של הממשלות ולכן ביכולת לחזות את תגובתן להרתעה. גל זה טען שחשיבה קיבוצית (Groupthink), תפיסות שגויות ופוליטיקה ארגונית עשויות להיות חזקות יותר מחישוב עלות-תועלת "קר". תפיסת הגל השלישי טענה שהרציונליות היא סובייקטיבית ולכן ההרתעה נסמכת על זיהוי הרציונל של המורתע. כמו כן, טענה תפיסה זו שחישוב של עלות-תועלת מתבסס על בהירות ועל מידה מסוימת של ודאות בנוגע לאופיו של העונש ולהפעלות וכמו כן גם על מידתיות העונש ביחס לעבירה. לכן, טענו תפיסות הגל השלישי שיש לבסס את מדיניות החוץ בכלל ואת מדיניות ההרתעה בפרט יותר על דיפלומטיה וחיזוקים חיוביים ופחות על איומים צבאיים.¹⁴⁶

עלייתם של שחקנים לא מדינתיים, של מדינות שאינן פועלות לפי כללי המשחק (Rouge States) ושל ארגוני טרור הביאה לגל הרביעי של תאוריות ההרתעה. שחקנים אלה אינם ניתנים להרתעה, כיוון שאינם נדרשים להגן על אזרחים או על שטח ולפיכך, כדי להתמודד עימם, נדרשים תקיפות מנע.¹⁴⁷

במהלך המלחמה הקרה ביססו האמריקנים, הרבה מההערכות שלהם בנוגע לכוונות הסובייטיות על האמל"ח הסובייטי, בלי להבין שהחל משנות ה-60 של המאה ה-20, דרישות האמל"ח ופיתוחו הוכתבו במידה הולכת וגדלה על ידי התעשייה הביטחונית הסובייטית ולא על ידי הכוחות המזוינים – ולכן, אי אפשר היה להעריך כוונות אסטרטגיות ותוכניות מבצעיות על בסיסו. פער הבנה אמריקני זה תרם לתפיסה של ברה"מ כבעלת כוונות אגרסיביות יותר ויכולות צבאיות טובות יותר מאשר היו לה במציאות.¹⁴⁸

נטען שהסיכונים שבהשמדה ההדדית הוודאית היו כה גבוהים וכה ברורים, עד שההרתעה הגרעינית לא באמת נבחנה בין ראשית שנות ה-60 של המאה העשרים ועד שנות ה-80 של אותה המאה. הסיכונים הוודאיים הללו נשענו על חוסר הודאות שבנטרול יכולות היריב ולכן על

¹⁴⁶ Lawrence Freedman, *Op. cit.*, p. 22-23; Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 5

¹⁴⁷ Annegret Bendiek, Tobias Metzger, *Op. cit.*, p. 5

¹⁴⁸ John G. Hines, Ellis M. Mishulovich, John F. Shull, *Soviet Intentions 1965-1985 Vol. 1 – An Analytical Comparison of US-Soviet Assessments During the Cold War*, Mclean, VA: BDM Federal Inc. (for OSD-Office of Net Assessment), 22 Sept. 1995, pp. 6-7

הסכנה המתמדת לתגובה הרסנית מצידו. אפשר שאי הודאות (שנשענה על יכולת ודאית) היא שעמדה בבסיס ההרתעה.¹⁴⁹

בכל מהלך המלחמה הקרה (ולאחריה) עוררה תפיסת ההרתעה מגוון של ספקות בנוגע לתקפותה במגוון תרחישים – לדוגמה, בהגנה על בעלי ברית, אל מול יריב בעל יכולות שוות ערך, על פני משך זמן ארוך וכו'. באופן כללי נחשבה ההרתעה המרכזית – הרתעה מפני חילופי מהלומות גרעיניות בין המעצמות – לאמינה יותר מאשר ההרתעה המורחבת ("המטריה הגרעינית" שאמורה להבטיח את שלום בעלי הברית). זאת משום שהתקפה על שטחן של ארה"ב או ברה"מ נחשבה לפגיעה באינטרס מרכזי, שתאפשר הפעלת נשק גרעיני ותצדיק אותה. מנגד, פגיעה בבעלי ברית עשויה שלא הייתה להספיק כדי להפעיל נשק גרעיני, על אחת כמה וכמה מול איום במכה גרעינית כתגובה. בהדרגה, העיסוק בהרתעה הגרעינית החל להיות מנותק מהמציאות. אי הודאות ואי היציבות התמידית שבהרתעה (הטמונה באפשרות להסלמה חסרת שליטה, אפילו כתוצאה משגיאות מיקרו-טקטיות) הביאו לחשש מההסתמכות הנרחבת על ההרתעה הגרעינית המוחלטת. חשש זה הוביל לניסיונות לצמצם את ההרתעה הגרעינית, בין אם על ידי הסכמי פירוק נשק ובין אם על ידי פתרונות הגנתיים (כגון תוכנית ה-SDI).¹⁵⁰

לאחר המלחמה הקרה, תפיסת ההרתעה הגרעינית המוחלטת איבדה ממקומה כיוון שכבר לא היה יריב משמעותי דיו כדי להרתיע באמצעות נשק גרעיני מוחלט. את ההרתעה של יריבים קטנים יותר בעלי ארסנל מוגבל של נשק גרעיני אמורים היו להשיג באמצעות מערכות הגנה נגד טילים, שיעקרו למעשה את הארסנל הקטן שבידי יריבים אלה. מנגד, ארה"ב גילתה כי הרתעה קונבנציונלית אי אפשר היה עוד להשיג באמצעות נשק גרעיני או אף בכלל (במקרה של אויבים אידיאולוגיים ולא מדינתיים) ולכן היא נדרשה לעבור לאסטרטגיה של מניעה. לאחר ה-11 בספטמבר 2001, עברה ארה"ב מגישה של הרתעה (שהניחה שאיום השימוש בכוח יכול להכיל התנהגות עוינת) לגישה של מניעה, שהניחה שיש איומים שאי אפשר להרתיע ולכן יש לאמנעם לפני שיתגשמו.¹⁵¹

ההרתעה במזרח

במהלך המלחמה הקרה, היו מקבלי ההחלטות הסובייטיים משוכנעים כי האמריקנים מתכננים למכה גרעינית ראשונה, למרות שהאמריקנים נקטו במדיניות של הרתעה גרעינית, והכריזו על כך פעמים רבות. כדי להבטיח את הישרדות המשטר הסובייטי, את ביטחון ברה"מ ואת ההשפעה הסובייטית באירופה ובעולם, נקטה ברה"מ במדיניות של הגעה לעליונות גרעינית

¹⁴⁹ Lawrence Freedman, *Op. cit.*, p. 18

¹⁵⁰ Lawrence Freedman, *Op. cit.*, pp. 18-19, 21, 35

¹⁵¹ Lawrence Freedman, *Op. cit.*, pp. 2, 20-21, 24

אל מול ארה"ב, תוך כדי מדיניות של מכה גרעינית מקדימה במקרה שארה"ב עומדת להפעיל נשק גרעיני – למרות הבנה ברורה כי ניצחון במלחמה גרעינית (כלשהיא, אפילו זירתית) אינו אפשרי. התפיסה הסובייטית נבעה מפירוש ייחודי לבניין כוח אמריקני (כגון פיתוח יכולות MIRV¹⁵² מדויק, שיפור דיוק הנשק הגרעיני האמריקני, פריסת מגוון רב של יכולות גרעיניות טקטיות באירופה, פיתוח טילי שיוט ארוכי טווח ועוד), לנקודות התורפה האמריקניות (כגון הפגיעות של מערך הטילים הבליסטיים הבין יבשתיים של ארה"ב למכה גרעינית), להכרזות אמריקניות (כגון הסירוב להכריז על דוקטרינה של הימנעות ממכה ראשונה) וכמו כן מהניסיון ההיסטורי הסובייטי הייחודי – בייחוד הפחד ממתקפת פתע, כפי שקרה בפתיחת מלה"ע 2. החיבור של יכולות, הכרזות, תורפות וניסיון היסטורי (רלוונטי ולא רלוונטי) יצר אצל מקבלי ההחלטות הסובייטיים תמונת עולם שונה מזו אותה ביקשו להנחיל האמריקנים והניעה אותם לעבר מרוץ חימוש אדיר מימדים, בניסיון להגיע לעליונות על ארה"ב.¹⁵³

בתגובה למדיניות הגרעינית האמריקנית, נקטו הסובייטים גם הם במדיניות הרתעתית, לפחות מאז סוף שנות השישים של המאה העשרים. בשונה מהאמריקנים שניסו לפתח יכולת הרתעה באמצעות היכולת לנהל מלחמה גרעינית, נקטו הסובייטים בתפיסה פשוטה של הרתעה על ידי הפעלה מאסיבית של נשק גרעיני.¹⁵⁴ מדיניות זו התבססה על איום ענישה גרעינית מאסיבית על מטרות אסטרטגיות (הן אזרחיות והן צבאיות) במקרה שנראה שהאויב עומד להפעיל נשק גרעיני או מיד לאחר שעשה זאת.¹⁵⁵

ההרתעה הסובייטית השתנתה לאורך השנים. עד שנות השבעים היא התבססה בעיקר על איום בתקיפה מקדימה מניעתית ולאחר שנות השבעים, במידה הולכת וגוברת, על תגובה גרעינית. מדיניות המכה המקדימה הייתה פועל יוצא של יכולת טכנולוגית – בשנות השישים והשבעים הצריכה הכנת הטילים לתקיפה בין 7 ל-9 שעות, ולא התאימה למשך הזמן הנדרש לתגובה מרגע גילוי תקיפה אמריקנית – על אחת כמה וכמה בהינתן היעדר יכולת השרידות של מערך הפו"ש הגרעיני הסובייטי. היעדר האמון ביכולת תגובה, דחף בניין כוח שתעדף כמות רש"קים על פני שרידותם (לדוגמה, באמצעות בניין יכולת טילי קרקע-קרקע ניידים או מיגון מאסיבי של מתקני שיגור חפורים). הדבקות בהרתעה על ידי תקיפת מנע הייתה בולטת יותר בדור מקבלי ההחלטות שחווה את מלה"ע 2 ואת התקפת הפתע הגרמנית וראה בהרתעה על

¹⁵² Multiple Independently targetable Reentry Vehicles – טכנולוגיה המאפשרת הרכבת מספר ראשי קרב על כל טיל, כאשר לכל רש"ק מטרה אחרת.

¹⁵³ John G. Hines, Ellis M. Mishulovich, John F. Shull, *Op. cit.*, pp. 1-2

¹⁵⁴ בשנות השישים המוקדמות נראה שמדובר היה במכה מקדימה גלובלית ואילו בשנות השבעים המוקדמות והלאה נראה שהתפיסה הסובייטית דגלה בניסיון להגביל כל מלחמה גרעינית לזירה אירופאית בלבד ולא ליזום הסלמה לרמה הגלובלית (אלא רק להגיב על הסלמה שכזו). עם זאת, ככל הנראה, מראיונות שנערכו לאחר המלחמה הקרה עם בכירים לשעבר במנגנונים הסובייטיים, נראה שהתגובה הגרעינית הסובייטית בכל מקרה לא הייתה אוטומטית ותקיפה גרעינית אמריקנית מוגבלת עשויה הייתה לקבל מענה גרעיני סובייטי מוגבל גם כן.

¹⁵⁵ John G. Hines, Ellis M. Mishulovich, John F. Shull, *Op. cit.*, pp. 2-3, 15, 16, 73-74

ידי איום בתגובה כתפיסה פאסיבית, המוותרת על היוזמה. רק בשנות השבעים, כאשר הבשילו מספר כיווני בניין כוח סובייטיים (חיזוק מיגון מתקני השיגור, הגדלת כמות הטילים במלאי, שיפור מערכות הפיקוד, השליטה והגילוי, פיתוח יכולת לשינוי מהיר של מטרת הטיל לפני השיגור וצמצום חד של זמן השיגור לסביבות דקה אחת), יכלו הסובייטים לעבור לתפיסת הרתעה על בסיס מכה שניה (בהתחלה "שיגור בעת התראה" ולבסוף "שיגור בתנאי התקפה"). מגמה זו הביאה בסופו של דבר לזניחת תפיסת התקיפה המקדימה (והמלחמה הגרעינית הגלובלית) כליל בשנת 1980 ולאימוץ התפיסה שיש להסתמך על הרתעה ומניעת מלחמה ולנהל מלחמה גרעינית מוגבלת בלבד במקרה הצורך (ולא מלחמה גרעינית טוטאלית וגלובלית, כפי שהאמינו בשנות השישים). בשנת 1981 זנח הדרג המדיני הסובייטי באופן רשמי גישת התקיפה המניעתית ועד אמצע שנות השמונים אומצה גישת התגובה (למרות שהצבא לא זנח לעולם את גישת התקיפה המניעתית, מתוך ספקות מסוימים ביכולת השרידות של המערך הגרעיני הסובייטי).¹⁵⁶

החשיבה הרוסית על הרתעה הייתה מורכבת הרבה פחות מזו האמריקנית (ולא כללה כל מיני פיתוחים כגון הסלמה מתוכננת ומכוונת וכו'). מדיניות זו לא יצאה מנקודת הנחה שאפשר יהיה לנהל מלחמה גרעינית (באמצעות מדרגות הסלמה, לדוגמה), להגבילה לרמה האזורית (בשונה מהאמריקנים) או אפילו לשרוד אותה. כיוון שלדעתם הרתעה לא נבעה ממאזן הדדי, אלא מעליונות ברורה, הם לא ביקשו לשמור על מאזן גרעיני, אלא לפתח עליונות גרעינית ובנו את כוחותיהם הגרעיניים בהתאם. למרות שמנהיגי ברה"מ לא האמינו בסיכוי לנצח מלחמה גרעינית, הם בנו נשק שהיה סביר שיופעל וכך שמרו על אמינות ההרתעה. עם זאת, נראה שגם המחשבה הגרעינית הסובייטית התפתחה מהתפיסה הטוטאלית המוקדמת שלה, כדי לאפשר ניהול מלחמה. כך, אחרי שהגיעו לסוג של מאזן גרעיני, באמצע שנות ה-70, החלו הסובייטים להשתמש בהרתעה גרעינית טקטית כדי לאפשר להם להניא את ברית נאט"ו מליזום מהלומה גרעינית טקטית במהלך מלחמה מוסכמת (קונבנציונלית) באירופה וכך למנוע מהמלחמה להפוך לגרעינית כלל.¹⁵⁷

אף כי נערכו הכנות נרחבות למלחמה גרעינית (ולשיקום האפשרי שלאחריה), מבחינה צבאית ופוליטית, ניסה הצבא הסובייטי להימנע ככל יכולתו ממלחמה גרעינית. החל מראשית שנות השבעים חילחלה בצבא הסובייטי הבנה שהשימוש הצבאי בנשק גרעיני (בשונה מהתועלת הפוליטית מהם) מוגבל ועד 1981 הבשילה הבנה זו לכדי פיסה ששימוש בנשק גרעיני יהיה קטסטרופלי ומזיק מבחינה צבאית ולכן יש להימנע ממנו ככל האפשר. בהתאם, הצבא הסובייטי כלל לא פיתוח הגדרה של ניצחון במלחמה גרעינית והתרכז בניסיון לגרום נזק גדול

¹⁵⁶ Ibid, pp. 28-29, 32-34, 75-76

¹⁵⁷ John G. Hines, Ellis M. Mishulovich, John F. Shull, *Op. cit.*, pp. 2-3, 15, 16

ככל האפשר ליריב. כמו כן, היו בכירים סובייטים שטענו, לאחר המלחמה הקרה, שההנהגה הסובייטית מעולם לא דנה בתקיפה גרעינית ראשונה¹⁵⁸ כנגד המערב (למרות קיומם של כתיבה ותרגילים צבאיים בנושא), נמנעה מהחלטה אישור שימוש בנשק גרעיני במהלך דיונים על מקרים ותגובות ומאז 1972 אף לא השתתפה בתרגילים שכללו שימוש בנשק גרעיני. זאת בשונה מהתפיסה האמריקנית בחלק מהמלחמה הקרה, שטענה שהסובייטים אינם ששים להתחיל במלחמה גרעינית, אך מאמינים ביכולתם לנצח במלחמה שכזו מרגע שתתחיל (ותפיסה קיצונית אף יותר של מיעוט מקרב האנליסטים האמריקנים לפיה הסובייטים מוכנים להתחיל מלחמה שכזו ומצפים לנצח בה).¹⁵⁹

במהלך המלחמה הקרה תפסו הסובייטים את ההרתעה הגרעינית שלהם שלהם במונחים של "לא לאפשר לארה"ב לעשות...". – לא לאפשר לארה"ב להאמין שהיא תוכל לתקוף את ברה"מ ללא תגובה הרסנית, לא לאפשר למנהיגים האמריקניים לחוש תחושת ביטחון ועליונות שתאפשר להם לנסות ולעשות ככל העולה על רוחם באירופה ולא לאפשר לארה"ב לחוש תחושת עליונות כה גדולת שתאפשר לה לנסות וליישם מדיניות הרפתקנית בעולם השלישי. בשונה מהמערב, הסובייטים תפסו את מאזן ההשמדה ההדדי כמצב לא יציב מבחינה אינהרנטית, כיוון ששינויים טכנולוגיים (כגון שיפור דיוק הנשק הגרעיני) או גודל הארסנל הגרעיני יכולים לשנותו ולגרום לצד זה או אחר להשיג עליונות. לפיכך, הם ביקשו להגיע לעליונות גרעינית מובהקת. כמו כן, בעוד שההשמדה ההדדית הייתה אפשרית תיאורטית, תפסו הסובייטים שיסנם הבדלים בין התיאוריה לבין המעשה הצבאי ולפיכך אפשר שבזמן אמת, כלל לא תיערך מכת תגובה גרעינית. לפיכך, התפיסה הגרעינית הסובייטית הייתה לתקוף תמהיל של יעדים – ערים, מרכזים תעשייתיים ומרכזים צבאיים. הרכב התמהיל אמור היה להשתנות בהתאם למצב – אם התקיפה הייתה מקדימה או תגובה. במקרה של תקיפה מקדימה, עיקר המטרות יהיו היכולות הגרעיניות של המערב (כולל אמצעי השיגור והשילוח כגון בסיסי אוויר וים) ואילו אם התקיפה הייתה כתגובה, עיקר המטרות יהיו מטרות צבאיות רכות (כגון מוצבי פיקוד ושדות תעופה) ותשתיות אזרחיות, כולל ערים.¹⁶⁰

כיוון שלסובייטים היה ספק בנוגע לשרידות המערך הגרעיני שלהם לאחר תקיפת פתע¹⁶¹, הם השקיעו משאבים רבים תחילה בהגדלה משמעותית מאוד של מספר ראשי הקרב הגרעיניים שלהם ולאחר ההגעה לעליונות מספרית, בשרידות מערכת הפו"ש. הדאגה הסובייטית ממתקפת פתע כנגד ההנהגה הסובייטית מודגשת על רקע מגוון הפיתוחים שלהם להבטיח

¹⁵⁸ בשונה מהתקפה גרעינית מקדימה

¹⁵⁹ John G. Hines, Ellis M. Mishulovich, John F. Shull, *Op. cit.*, p. 23-26

¹⁶⁰ John G. Hines, Ellis M. Mishulovich, John F. Shull, *Op. cit.*, pp. 15-18

¹⁶¹ לפי הנחותיהם – לאחר מתקפת פתע גרעינית, תוכל ברה"מ לשגר בין 10%-20% מהארסנל הגרעיני שלה, בעיקר עקב בעיות שרידות של מערך הפו"ש הגרעיני.

שיגור מוצלח של הארסנל הגרעיני שלהם במקרה של מתקפה כזו – כולל טילים שרידים במיוחד המורים על שיגור טילים נוספים עם שיגורם ולבסוף גם ניסיון¹⁶² לפתח מנגנון שיגור אוטומטי ברובו (Dead Hand).¹⁶³ מכאן, לסובייטים הייתה תפיסת איום ייחודית, שונה מזו האמריקנית אך במידה מסוימת גם דומה לה, שהתכתבה איתה במובנים מסוימים, אך הושפעה מאוד מהתרבות וההיסטוריה הרוסית. התפיסה הזו וההיבטים התרבותיים שבה הקשו לעיתים על ההבנה האמריקנית של תפיסת האיום עצמה ושל מעשי הסובייטים ומטרותיהם באופן כללי (אף כי, ככל הנראה, באופן כללי הצליחו האמריקנים להבין באופן מדויק את החשיבה הסובייטית).

ברה"מ ביקשה ליצור הרתעה מפני תקיפה גרעינית על ידי כך שאמרה בפומבי שתגיב במתקפה גרעינית מסיבית על כל הפעלה של נשק גרעיני נגדה – ללא קשר לגודלה. הבהירות שבמסר והטוטאליות שלו נועדה להרתיע. עם זאת, התקיפה הגרעינית לא הייתה אוטומטית והייתה אמורה להתקבל על ידי הפוליטבורו – שלא היה ברור האם באמת יחליט להסלים תקיפה מוגבלת לכדי מלחמה גרעינית טוטאלית (אבל אי אפשר היה להניח שלא יסלימו).¹⁶⁴

¹⁶² שהושלם או שלא

¹⁶³ John G. Hines, Ellis M. Mishulovich, John F. Shull, *Op. cit.*, pp. 18-19

¹⁶⁴ John G. Hines, Ellis M. Mishulovich, John F. Shull, *Op. cit.*, p. 37

רשימת מקורות

- Andrew S. Swiss, Richard Nephew, **The Role of Sanctions in US-Russian Relations**, Carnegie Endowment for International Peace, 11 Jul. 2016, www.carnegieendowment.org/2016/07/11/role-of-sanctions-in-u.s.-russian-relations-pub-64056
- Annegret Bendiek, Tobias Metzger, **Deterrence Theory in the Cyber-Century**, Working Paper RD EU/Europe 2015/02, Berlin: German Institute for International and Security Affairs, May 2015
- **Assessing Russian Activities and Intentions in Recent US Elections**, ICA 2017-01D, Washington, DC: Office of the Director of National Intelligence, 06 Jan. 2017, www.dni.gov/files/documents/ICA_2017_01.pdf
- Benjamin Runkle, "The Best Strategy for Cyber-Conflict May Not Be a Cyber-Strategy", **War on the Rocks**, 08 Nov. 2016, www.warontherocks.com/2016/11/the-best-strategy-for-cyber-conflict-may-not-be-a-cyber-strategy/
- Brian Krebs, "The Download on the DNC Hack", **Krebs On Security**, 03 Jan. 2017, www.krebsonsecurity.com/2017/01/the-download-on-the-dnc-hack
- Christopher A. Bartos, "Cyber Weapons are Not Created Equal", **USNI Proceedings Magazine**, Vol. 142/6/1, June 2016
- Clorinda Trujillo, "The Limits of Cyberspace Deterrence", **JFQ** 75, 4th Quarter, 2014
- Dan Goodin, "White House Fails to Make Case That Russian Hackers Tampered with Elections", **Ars Technica**, 31 Dec. 2016, www.arstechnica.com/security/2016/12/did-russia-tamper-with-the-2016-election-bitter-debate-likely-to-rage-on

- Danny Vinik, "America's Secret Arsenal", **Politico**, 10.12.2015, <http://www.politico.com/2015/12/defense-department-cyber-offense-strategy-00331>
- David D. Clark, "Untangling Attribution", in: Committee on Deterring Cyberattacks, **Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy**, Washington, DC: National Research Council, 2010
- Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?", **Journal of Strategic Security**, Vol. 7 No. 1, 2014
- Eric Sterner, "Retaliatory Deterrence in Cyberspace", **Strategic Studies Quarterly**, Spring 2011
- **Executive Order – "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"**, 01 Apr. 2015
- Forrest E. Morgan et. al., **Dangerous Thresholds – Managing Escalation in the 21st Century**, Santa Monica, CA: RAND, 2008
- Franklin D. Kramer and Aelanie J. Teplinsky, **Cybersecurity and Tailored Deterrence**, Atlantic Council, Dec. 2013
- **Grizzly Steppe – Russian Malicious Cyber Activity**, JAR-16-20296A, 29 Dec. 2016, www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf
- John G. Hines, Ellis M. Mishulovich, John F. Shull, **Soviet Intentions 1965-1985 Vol. 1 – An Analytical Comparison of US-Soviet Assessments During the Cold War**, Mclean, VA: BDM Federal Inc. (for OSD-Office of Net Assessment), 22 Sept. 1995

- Jonathan F. Solomon, "Demystifying Conventional Deterrence – Great Power Conflict and East Asian Peace", **Strategic Studies Quarterly**, Winter 2013
- Kelly Jackson Higgins, "Mandiant: Russian State Hackers Changed the Game", **Dark Reading**, 01 Dec. 2016, www.darkreading.com/threat-intelligence/mandiant-russian-state-hackers-changed-the-game-/d/d-id/1327616
- Laura K. Bate, "In Search of Cyber Deterrence", **War on the Rocks**, 24 Sept. 2015, www.warontherocks.com/2015/09/in-search-of-cyber-deterrence
- Lawrence Freedman, **Deterrence**, Cambridge: Polity Press, 2004
- Leo Miri, "Worrying About Cyber War Is Making Us Less Safe", **Defense One**, 3 Dec. 2014, <http://www.defenseone.com/technology/2014/12/worrying-about-cyber-war-making-us-less-safe/100424/>
- Liam Nevill, Zoe Hawkins, **Special Report: Deterrence in Cyberspace – Different Domain, Different Rules**, Berton Australia: Australia Strategic Policy Institute, July 2016
- Lorenzo Franceschi-Bicchieri, "The Declassified Report on Russia's Election Hacking Says Nothing New", **Motherboard**, 7 Jan. 2017, www.motherboard.vice.com/en-us/article/the-declassified-report-on-russias-election-hacking-says-nothing-new
- Mark Hosenball, "British Hacker for Islamic State Killed in US Drone Strike in Syria: Sources", **Reuters**, www.reuters.com/article/us-mideast-crisis-hacker-isUSKCN0Qv2KA20150827

- Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy", **Strategic Studies Quarterly**, Winter 2012
- Matthew D. Crosston, "World Gone Cyber MAD – How Mutually Assured Debilitation Is the Best Hope for Cyber Deterrence", **Strategic Studies Quarterly**, Spring 2011
- P. W. Singer, "How the United States Can Win the Cyberwar of the Future", **Foreign Policy**, 18 Dec. 2015, <http://www.foreignpolicy.com/2015/12/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/>
- Patrick Cirenza, "The Flawed Analogy between Nuclear and Cyber Deterrence", **Bulletin of the Atomic Scientists**, 22 Feb. 2016, <http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179>
- Patrick Cirenza, **An Evaluation of the Analogy Between Nuclear and Cyber Deterrence**, Stanford University, June 2015
- Robert M. Lee and Thomas Rid, "OMG Cyber!", **RUSI Journal**, 159:5
- Susan Hennessey, "Is US Cyber Deterrence Strategy More than (Russian) Roulette?" **Lawfare**, 12 Oct. 2016
- Tang Lan and Zhang Xin, "Can Cyber Deterrence Work?", in: Andrew Nagorski (ed.), **Global Cyber Deterrence – Views from China, the US, Russia, India and Norway**, New York: The East-West Institute, April 2010
- Tyler Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options", in: Committee on Deterring Cyberattacks, **Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy**, Washington, DC: National Research Council, 2010
- **Wales Summit Declaration**, 05 Sept. 2014. www.nato.int/csp/en/natohq/official_text_112964.htm

- Will Goodman, "Cyber Deterrence – Tougher in Theory than in Practice?", **Strategic Studies Quarterly**, Fall 2010.