המרחב הקיברנטי וארגוני הטרור

יורם שווייצר, גבי סיבוני ועינב יוגב

מבוא

באחת הסצנות בסרט "מת לחיות 2" (ארצות־הברית 1990) משתלטים טרוריסטים על מערכות המחשוב, בקרת התעבורה, והתקשורת האווירית, מתחזים לפקחי טיסה, נותנים נתונים כוזבים ובתוך סופת שלגים מנחים את טייסי המטוס ויושביו להתרסקות קטלנית על מסלול הנחיתה. לא היה ביכולתם של גורמי הביטחון לתת מענה וסיוע, וגיבור הסרט ג'ון מקליין (בגילום ברוס ויליס), נותר חסר אמצעים להושיע מלבד עמידה חסרת תכלית בערפל על מסלול הנחיתה ונפנוף לעברו של המטוס בשני לפידים מאולתרים. לכאורה מדובר בעוד פנטזיה הוליוודית שאפשר לבטלה כגוזמה, וזו אף שודרגה בסרט המשך – "מת לחיות 4". ואולם פיגועי ה־11 בספטמבר 2001, והשינויים וההתפתחויות באיומים הביטחוניים בעשור האחרון, מצביעים על כך שגם התסריטים הדמיוניים ביותר שנרקמו באולפני הוליווד, יכולים למצוא ביטוי מעשי במרחב הציבורי והביטחוני של ימינו.

השימוש במרחב הקיברנטי כזירה מרכזית ללוחמה בין אויבים או בין מדינות יריבות היה מאז ומעולם קרקע פורייה לפנטזיות ולסצנות מרהיבות בקולנוע. ואולם מרחב זה, ששימש בעבר תפאורת רקע לסצנות מלחמה הוליוודיות, הולך ותופס מקום מרכזי כזירה חשובה, שבה, כך מסתמן, ינוהלו מלחמות העתיד, וכאחת הזירות שיתבצעו בה פעולות עוינות בין גורמים יריבים. יש אפשרות שבין גורמים אלה יימצאו גם ארגוני טרור, שעד כה השתמשו בעיקר בפעילות פיזית אלימה כדי לקדם את האינטרסים שלהם, ולעתים גם את אלו של שולחיהם. נוכח איומים אלו, הקימו מדינות במערב בשנים האחרונות רשויות מיוחדות שנועדו להיערך לקראת פעולות לוחמניות תוך שימוש באמצעים טכנולוגים חדשניים נגד יעדי תשתית אסטרטגיים. מאמר זה מתמקד בניתוח היתרונות והמגבלות העלולים להביא לידי כך שארגוני טרור ישתמשו בכלים קיברנטיים כדי לתקוף תשתיות קריטיות של

יורם שווייצר עומד בראש פרויקט הטרור במכון למחקרי ביטחון לאומי אל"מ (מיל.) ד"ר גבי סיבוני הוא ראש תכנית צבא ואסטרטגיה ותכנית לוחמה קיברנטית, הנתמכת על ידי קרן ג'וזף וג'נט ניובאוואר, פילדלפיה, ארצות הברית
עינב יוגב היא עוזרת מחקר בפרויקט הטרור במכון למחקרי ביטחון לאומי

מדינות, מוסדות וסמלי שלטון, תשתיות ומערכות עסקיות ותעשייה, וכן יעדים אזרחיים ציבוריים למיניהם. כן נבחן האם מדובר באיום ממשי ומידי, או שמא זהו איום פוטנציאלי רחוק, השב ועולה מעת לעת כחלק מהשיח הכללי בתחום זה.[1]

האיום הקיברנטי מצד קבוצות טרור

חמש קבוצות עיקריות משתמשות כיום, או שיש להן פוטנציאל לשימוש בעתיד, בכלי תקיפה קיברנטיים: (1) מדינות המפתחות יכולות התקפיות והגנתיות כחלק (גדל והולך) מיכולות הפעלת הכוח שלהן; (2) גורמים פליליים המונעים בעיקר מאינטרסים פליליים־עסקיים; (3) חברות עסקיות הפועלות בעיקר בתחום ההגנתי מכיוון שהיקף ההתקפות במרחב הקיברנטי בהקשרים עסקיים גדל והולך במידה ניכרת, אולם חלק מהן עלולות לפנות לאפיק של התקפה על חברות מתחרות; (4) ארגוני טרור, שמשום היתרונות הגלומים בשימוש במרחב זה ומשיקולי עלות־תועלת בעבורם עלולים לנסות ולבצע התקפות טרור קיברנטי; (5) גורמים "אנרכיסטיים", המתנגדים למערכת הממסדית הקיימת, מעוניינים לחבל בה מבפנים או מבחוץ, ויבקשו לתקוף את מערכת המחשוב, שהיא כיום הבסיס לניהולה, בכוונה לשבש ואף להרוס את הסדר החברתי ואת מרקם החיים במדינה.

תחום התקיפה הקיברנטית, שאליו עלולים להיכנס ארגוני הטרור נושא בחובו פוטנציאל לשינוי במאזן הכוחות בחברה, משום העוצמה שהוא מעניק לתוקפים, ובייחוד לארגוני טרור הפועלים בנחיתות ביחסי הכוחות הא־סימטריים בינם לבין יריביהם. בניית יכולת במרחב הזה עשויה לאפשר להם לתקוף מתקנים, תהליכים מערכתיים ואתרים של יריבים ולגרום נזקים פיזיים כבדים וליצור השפעה פסיכולוגית ניכרת בחברה ובציבור המותקפים, וזה תוך כדי יכולת פעולה בממדים נוספים על אלה המוכרים לנו כיום מפעולות הטרור הקונבנציונליות, כגון פיגועי התאבדות, הפעלת מטעני חבלה, התבצרות עם בני ערובה, חטיפות כלי תעבורה ובני אדם. לתקיפה קיברנטית יש כמה יתרונות: ראשית, הימנעות מנוכחות פיזית ביעד המותקף. אפשר לנסות ולפגוע מרחוק ברשתות תקשורת ובמערכות בקרה של מתקנים ותהליכים וכך להימנע מהצורך להתמודד עם מכשולים פיזיים ומערכות אנושיות. שנית, היקף הנזק – תקיפה קיברנטית איננה מתקיימת בחלל פיזי בלבד אלא יש לה פוטנציאל לפגיעה קשה ומתמשכת במערכות בקרה ותשתית. בעוד רוב פיגועי הטרור מתוחמים בזמן ובמקום,[2] הפיגוע הקיברנטי מעצים את היבטי החרדה וההפחדה הכרוכות בהשפעות הפסיכולוגיות של מעשה הטרור. שלישית, טשטוש זהויות ומקור ההתקפה – במרחב הקיברנטי קל יותר לעמעם ולטשטש זהויות וגבולות שבין מדינות. גורמי הטרור יכולים לתקוף קיברנטית תוך כדי טשטוש זהויות וביצוע הטעיות לגבי מקור התקיפה. למשל, לתקוף בתוך מדינת היעד תוך כדי שימוש בכתובות של מדינה ידידותית. כך יתקשה המותקף

לזהות את המקור האמיתי של התקיפה. רביעית, יחס עלות־תועלת מיטבי – השימוש בפלטפורמה קיברנטית לצורכי תקיפות טרור מגלם יחס עלות־תועלת מיטבי מבחינתו של ארגון הטרור, שהוא נחות ברמת המשאבים והיכולות לעומת המדינות שאותן הוא תוקף. בהנחה שארגוני טרור יעדיפו מטרות מוגנות פחות על פני אלה המוגנות היטב, הרי שהם יוכלו לתקוף תוך כדי יצירת נגישות על־ידי החדרת מפגעים שיחדירו קודים זדוניים לאתרי היעד, או תוך שימוש בטכנולוגיה העומדת להיות זמינה למדי לקהלים רחבים. חמישית, טרור אל־הרג – באמצעות תקיפות קיברנטיות יכול ארגון הטרור לגרום נזקים ניכרים בלי פגיעה פיזית והרג ישיר. כך הוא יוכל להשיג הישגים באמצעות הפחדה ושיבוש מרקם החיים בלבד, דבר שיעניק למבצעיו יכולת הגנה והסבר לוגי למעשיהם בלי ששפכו דם אלא רק גרמו לנזק בדמים. חדשנות הפעולה תבטיח אף היא פרסום רב לארגוני הטרור, ואף כניסה לתחום פיגועי מיקוח־אל־הרג, שלאחר הדגמות ידרשו תמורות באיימם בפגיעה קיברנטית.

מושמעת טענה שארגוני טרור אינם מעוניינים במרחב הקיברנטי משום שהם מעדיפים פעולות ראוותניות של שפיכות דמים, בעלות נראות גבוהה בהרבה מהאלמוניות המאפיינת כביכול פעולות חבלה באמצעות המרחב הקיברנטי.[3] ואולם טענה זו אינה מתיישבת עם התפיסה הבסיסית של השימוש באסטרטגיית הטרור, הגורסת שהפעילות הטרוריסטית צריכה להתמקד בניסיון לצמצם את פערי העוצמה במאבק עם יריב שעוצמתו רבה יותר, ביצוע פעולות הרסניות תוך כדי חיפוש נקודות תורפה במערכי ההגנה שלו כדי לחדור מבעדן, והשגת עמדת יתרון במחיר נסבל ההולם את האמצעים הדלים יחסית העומדים לרשות מחוללי הטרור. כבר היום אפשר לראות, שארגוני טרור מהג'יהאד העולמי עושים שימוש רב, אם כי מוגבל ועדיין לא מפותח יחסית, במרחב הקיברנטי כדי להביא יתרונות אלו לידי מימוש. במחקר שבחן את היכולת ואת השימושים בתחום הקיברנטי של ארגוני ג'יהאד,[4] נמצאו מאפיינים עיקריים המשמשים לבנייה ולשיפור התשתית הארגונית והמבצעית של ארגוני הטרור בתחומים האלה:

- **תעמולה** – שימוש לצרכי הפצת רעיונות, פסיקות, הנחיות, נאומים ודעות של אנשי דת ומנהיגי טרור;
- **גיוס ואימון** – שימוש לצורכי איתור וגיוס של חברים פוטנציאליים, וכן העברת חומרי הכשרה והדרכה באמצעות הרשת;
- **גיוס כספים ומימון** – שימוש ברשת לגיוס כספים במסווה של ארגוני צדקה וסיוע, ושימוש לגנֵבת זהויות וכרטיסי אשראי;
- **תקשורת** – שימוש ברשת כגורם לתקשורת מבצעית תוך שימוש בכלים מגוונים ובהם כלי הצפנה זמינים;

- **איתור מטרות ומודיעין** – שימוש במידע ברשת לשם איתור מטרות ומחקר מודיעיני.

המעבר של ארגוני הטרור משימוש לוגיסטי ותעמולתי לשימוש אופרטיבי באמצעים קיברנטיים עלול לבוא לידי ביטוי בביצוע פיגוע דרמתי וחדשני, זול למדי בעלותו אך עם תהודה רבה ולעתים עם נזק בהיקף גדול ביותר, אפילו אם נעשה בחתימה נמוכה או אפילו בשמירה על אנונימיות של מבצעיו. לכן כל ארגון טרור, ובעיקר אלה השואפים לפרסום וליצירת אפקט פסיכולוגי על ציבור יריביהם, רואה בפיגוע כזה אתגר חשוב ושאיפה ראויה, שכדאי להתאמץ בעבורו. חדשנות גם תבטיח למבצעים פרסום בינלאומי ואת היותם דגם לחיקוי. לפיכך ארגונים תת־מדינתיים שיכולתם הטכנולוגית נמוכה משל מדינות שבהן הם נאבקים, עלולים להצטרף למגמה של ניצול הטכנולוגיה המתקדמת הנדרשת ללוחמה הקיברנטית, בייחוד, אבל לא כתנאי הכרחי, אם יזכו לסיוע של מדינות תומכות או אם יצליחו לרכוש בעצמם יכולת כזאת בעתיד על־ידי גיוס אנשים בעלי הכשרה מתאימה בתחום הזה, שיוכלו להביא לידי ביטוי כישורים יוצאי דופן בתחום.

גם למדינות תומכות טרור יש במרחב הקיברנטי כוח משיכה רב להפעלת ארגוני שליח: האנונימיות הטמונה בשימוש כזה, הקושי להוכיח את זהות המפעיל, יכולת ההכחשה (deniability) הגבוהה של מדינות בנוגע למעורבותן נוחה יותר, והגמול בדמות גרימת הנזק הרב ליריב. יתר על כן, גם אם יעלה כלפיהן חשד, יהיה קשה להוכיח את אשמתן, ובכל מקרה "פיגוע קיברנטי" עשוי להיחשב מקומם פחות את הציבור הנפגע מפיגוע טרור בנשק חם הגורם שפיכות דמים גדולה, אפילו שהנזק בעטיו של הראשון רב ביותר, ואף עלול לעלות בהרבה על הנזק לרכוש ולחיי אדם הנגרמים מפעולת טרור אלימה ומדממת.

למרות היתרונות של תקיפה קיברנטית שתוארו לעיל, עדיין לא נודעה תקיפה שהאחראים לה הם גורמי טרור. בניית יכולת ממשית בתחום התקיפה הקיברנטית מחייבת מעבר של סף מודיעיני וטכנולוגי לא מבוטל. בשלב זה סביר להניח שלארגוני הטרור יש קושי לאתר, לגייס ולתחזק יכולת ונגישות טכנולוגית גבוהה ביותר המאפשרת להגיע לסף הזה. אמנם הישענות על יכולת של מדינות תומכות טרור עשויה לספק מענה ולו חלקי למגבלה זאת, אולם אין בה, לפחות בשלב הנוכחי, כדי לייצר לארגוני הטרור מצע טכנולוגי יציב ומשמעותי הנדרש לקיומה של יכולת תקיפה קיברנטית אפקטיבית. כן ניצבים ארגוני הטרור בפני מגבלות הפעילות במרחב הקיברנטי הגלוי (רשת האינטרנט). זהו חיסרון מובהק ואתגר לא מבוטל לארגוני טרור, שכן יכולת המעקב והמודיעין הקיברנטי של מדינות ומעצמות טכנולוגיות מאפשרת להן לזהות התנהגויות חשודות ברשת, לאתר התארגנויות ולהתגונן מפניהן ומפני איומים ספציפיים.

נקודות תורפה ומענים

אף־על־פי שעד כה לא הצליחו ארגוני הטרור להתגבר על המכשולים להשגת יכולת תקיפה קיברנטית, המערכות האזרחיות והפגיעה במרקם החיים השגרתי נותרו ככל הנראה היעדים המועדפים שלהם. אלו הן נקודות התורפה העיקריות, ויכולת הגנתן פחותה מזו של המערכות הביטחוניות. סביר להניח שחיזוק ההגנה על תשתיות לאומיות חיוניות דוגמת מערכות אספקת חשמל, מים ותקשורת, תוביל את ארגוני הטרור לנסות לפגוע ביעדים מוגנים פחות השייכים למגזר האזרחי והעסקי. אף שבמקרים רבים מערכות ממגזרים אלה אינן נכללות בקבוצת התשתיות הקריטיות המוגנות, הרי מבחינת ארגוני הטרור המתקפה יכולה לספק תוצאה אפקטיבית בעיקר בהיבטי הדימוי והפגיעה בביטחון הבסיסי של התושבים.

חלק נכבד בבניית מערך הגנה כנגד תקיפת סייבר הוא כללי ואינו תלוי במקור האיום, בין שמקורו בארגוני טרור, ובין שמקורו בגורמים מדינתיים או בגורמים פליליים. כך בהיבטים הארגוניים דוגמת הרשות לאבטחת מידע בישראל ומשרדים המתמחים בהגנת סייבר במדינות שונות, וכך בחלק ממרכיבי ההגנות מתחום מערכות המידע והאבטחה הכוללת. לעומת אלה, אל מול ארגוני טרור המבקשים להפעיל כלים קיברנטיים, נדרשים שני רכיבים ייעודיים, המחייבים פיתוח ושכלול מתמשך.

מודיעין – איסוף אקטיבי של מודיעין מדויק ואיכותי מחייב פעילות איסוף ממגוון מקורות ובהם מקורות גלויים, וממוחשבים ומרשתות של ארגוני הטרור. לצורך זה יש לפתח יכולות לשהות במערכות האלה בצורה סמויה ולהזרים מידע בצורה פעילה ומתמשכת. לשם כך יש להתגבר על הפרישה הגלובלית הרחבה המאפיינת את ארגוני הטרור, המשתמשים בחדרי דיונים רבים ברשת, ומעבירים מסרים במילות קוד ייחודיות. גורמי המודיעין נדרשים לבנות יכולת ליירט תשדורות אלה ולפענחן בקבועי זמן רלבנטיים, ובה בעת לספק לגורמי ההגנה הקיברנטית את הכלים להגן מפני הפעולות המתוכננות ואף לשבש אותן.

שיבוש – בשונה מהקמה של מערכות הגנה, שאינן מנסות למנוע את התקיפה אלא למנוע את הצלחתה, מטרת השיבוש היא לסכל את ביצוע התקיפה או לפגוע במהלכיה. הקמת מערך שיבוש אפקטיבי כנגד תקיפות קיברנטיות של ארגוני טרור מחייב ניטור ובקרה מודיעיניים שיוכלו לזהות את ההתארגנות לתקיפה טרם התרחשותה, ולפעול ביעילות לסיכולה. היבט זה נשען בעיקר על יכולת איסוף של מודיעין טקטי הן במחשבים והן ברשתות התקשורת שארגוני הטרור משתמשים בהן.

לעתים, נעשים ניסיונות שיבוש שאינם מופנים לכוונת תקיפה מסוימת, אלא כניסיון לפגוע בתשתיות הארגוניות של ארגון היעד. ניסיון כזה אירע למשל באנגליה כאשר המודיעין הבריטי השחית את גיליונו המקוון של כתב העת האנגלי

Inspire של ארגון אל־קאעדה. בנוסף, בשנים האחרונות הג׳יהאד האלקטרוני על מרכיביו מהווה יעד לתקיפות סייבר מזדמנות, שרובן מיוחסות לממשלות של מדינות מערביות: אתר הטאליבן הושחת חדשות לבקרים, וכן הותקפו פורומים ג׳יהאדיסטיים אקסקלוסיביים ואתרים פונדמנטליסטיים עתירי פרופיל. מנגד רשויות אמריקניות, סעודיות והולנדיות דולות מידע מודיעיני יקר ערך על אודות טרור אסלאמי פוטנציאלי מאתרים ג׳יהאדיסטיים המשמשים ״מלכודות דבש״ (honeytraps) למודיעין איכותי.[5]

בצד אלה חובה להעמיק את הגנת המערכות האזרחיות שהן נקודות התורפה הגדולות ביותר, ולכן הן המטרות המועדפות על ארגוני הטרור. ממשלת בריטניה למשל החלה לנקוט אמצעים חקיקתיים רבים הכוללים אישור שימוש באמצעים פולשניים, כגון ציטוט לשיחות טלפון, מעקבים אחרי תנועות דואר אלקטרוני בתיקים משטרתיים הקשורים לעברות טרור, טרפוד תהליכי רדיקליזציה דרך האינטרנט ואימון ייעודי של יחידות משטרה להתמודד עם איום סייבר.[6] עם זאת, ברוב המדינות ההגנה על המערכות האזרחיות עודנה בחיתוליה. עיקר משאבי המדינות בתחום ההגנה הקיברנטית מוקצים למערכות הביטחוניות ולמה שקרוי תשתיות לאומיות קריטיות. העמקת ההגנה על המערכות האזרחיות מחייבת שידוד מערכות לאומי, החייב להיתמך ברגולציה מתאימה.[7]

סיכום

במפגש שהתקיים בניו יורק בדצמבר 2001, זמן לא רב לאחר מתקפת הטרור בארצות־הברית, שטח הפילוסוף ז׳אק דרידה את תפיסתו על התמורות שחוללו בעולם פיגועי ה־11 בספטמבר 2001. לשיטתו פיגועים אלו הם עדיין חלק מ״תיאטרון האלימות העתיק״, העולם הממשי והנראה, שבו דברים עדיין מתנהלים ב״סדר ברור וגדול״. ואולם לדבריו, המרחב הקיברנטי מציב איום חמור יותר על עולמנו הפוליטי והפיזי – הסכנות הטמונות בו משנות את היחס בין טרור, במובן הפסיכולוגי וההיסטורי של התקפה אלימה, לבין המושג טריטוריה. כעת, בעידן הטכנו־מדעי החדש, האיום שהכרנו בעבר כממשי, נהפך לאיום בלתי נראה, שקט ומהיר ובלא שפיכות דמים, שלדברי דרידה הוא גרוע יותר מפיגועי ה־11 בספטמבר, שכוונו כלפי מקום ידוע בזמן מסוים. כעת אנו ניצבים נוכח אתגר המאיים על מרקם החיים החברתיים־הכלכליים, מרקם שכולנו קשורים ותלויים בו, בכל נקודה ובכל רגע.[8]

ההתפתחויות והחידושים הטכנולוגים המהירים בשנים האחרונות במרחב הקיברנטי אכן יצרו שדה לחימה שבו חוברות ומאוגדות להן בו בזמן אוכלוסיות מגוונות ורבות, מקומיות ובינלאומיות, שהן יעד נחשק לפעילותם של ארגונים תת־מדינתיים. נכון לעת הזאת טרם נודעה תקיפה קיברנטית של גורמי טרור ולכן

האיום אינו נראה מיידי. הגורמים הרוצים לנצל את המרחב הקיברנטי למטרות זדון צריכים לעבור סף גבוה בשלושה רכיבים חיוניים: השגת מודיעין איכותי, נגישות ויכולת לפצח מערכות מחשוב המוגנות בטכנולוגיה גבוהה, וכן כושר חישוב ומחשוב גבוהים. ואולם היתרונות שבהשגת היכולת הקיברנטית, שפורטו במאמר זה, עלולים לשמש להם תמריץ לפתח, לרכוש או לגייס יכולת כזאת בעתיד. השגת שליטה ביכולות הטכנולוגיות והמודיעיניות המתקדמות הנדרשות במרחב הקיברנטי, צפויה להעניק לגורמים כאלה יכולת לשבש את אורח החיים התקין של אוכלוסיות הנחשבות יריבות, לערער את אמונתן בממשליהן ותזכה אותם בעוצמה ובחשיפה תקשורתית שחשיבותן רבה. לפיכך חייבות מדינות המערב להתכונן בהתמדה כדי לקדם את פני הרעה הצפויה הזאת ולשפר את יכולת המודיעין ואת יכולת ההגנה על המערכות האזרחיות. בד בבד עליהן לבנות מודיעין מדויק ויכולת הגנה על המערכות הביטחוניות ועל התשתיות הלאומיות הקריטיות ויכולת לשבש התארגנויות ותקיפות קיברנטיות של ארגוני טרור. הפקרתו של המרחב הקיברנטי האזרחי, שהוא מטרה לארגוני טרור, עלולה להביא בעתיד לידי תוצאות הרות אסון, שבשעת מבחן יציבו את גורמי הביטחון, כמו את גיבור הסרט "מת לחיות 2", בנסותם להציל מטוסים מתרסקים כשבידיהם לפידים בוערים בלבד.

הערות

1 השימוש במינוח טרור קיברנטי במאמר זה הוא בהקשר של השימוש בכלים קיברנטיים העלול לשמש ארגוני טרור לצורך תקיפת תשתיות כלכליות ומערכות אזרחיות במדינות יעד.

2 אפשר להחריג כאן פיגועים דוגמת התקיפה ב־11 בספטמבר 2001 בארצות־הברית, שהשפיעה גלובלית על מערכי הבטיחות בתעופה.

3 שמואל אבן ודוד סימן־טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, המכון למחקרי ביטחון לאומי, מזכר 109, יוני 2011, עמ' 42.

4 *Examining the Cyber Capabilities of Islamic Terrorist Groups*, Institute for Security Technology Studies at Dartmouth College, Technical Analysis Group, March 2004.

5 Adam Rawnsley, "Stop the presses! Spooks hacked al-Qaida online mag," *Wired*, June 3, 2011, http://www.wired.com/dangerroom/2011/06/stop-the-presses-spooks-hacked-al-qaida-online-mag/June 4, 2011.

6 "Warning of rise in cyber-terrorism," *The Independent*, July 12, 2011, http://www.independent.co.uk/news/uk/crime/warning-of-rise-in-cyberterrorism-2312434.html, (July 14, 2011).

7 גבי סיבוני, "הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי", **צבא ואסטרטגיה**, כרך 3, גיליון 1, מאי 2011.

8 ז'אק דרידה, מתוך ג'יובנה בוראדורי, **פילוסופיה בזמן טרור – שיחות עם הברמאס ודרידה**, תל־אביב, הקיבוץ המאוחד, 2004, עמ' 173–174.