גיוס הטכנולוגיה למאבק בטרור

עוזי עילם

מבוא

במאה העשרים הייתה הטכנולוגיה מרכיב מרכזי בבניין הכוח לקראת המלחמות ובייחוד בהתמודדות הבין־גושית שלאחר תום מלחמת העולם השנייה. כיום הטרור הוא האיום העיקרי לעולם וברור שהמלחמה בו היא **המלחמה** שאליה צריך להיערך, ולכן חובה לראות בטכנולוגיה אבן בניין חיונית במלחמה זו. מדובר בהתמודדות עם טרור "פשוט", המשתמש בחומרי נפץ ובמתאבדים, אך גם בהתמודדות עם איום עתידי של טרור עתיר טכנולוגיה. כבר עתה יש שימוש בטכנולוגיה בשני צִדי המתרס: ארגוני הטרור משתמשים בדרך כלל בטכנולוגיות קיימות, שאותן הם יכולים להשיג בקלות יחסית, ואילו המדינות המתגוננות מפתחות טכנולוגיות מתקדמות ומשקיעות בהן מאמצים ותקציבים ניכרים.

ואולם במלחמה בטרור עדיין אין מיצוי הולם של היכולות הטכנולוגיות. נראה גם שההכנות בתחום זה סובלות מהעדר ניתוח והגדרה בהירים של איום הטרור, ומנטייה להגיב ולא להיות היוזם בבניית היכולת של לחימה בטרור. אין די בהערכת מצב סטטית ובתיאור, ברור ככל שיהיה, של ההווה. נדרשת צפייה אל איומי העתיד והתמקדות בפתרונות עתידיים ובטכנולוגיות שעדיין אינן בהישג יד.

במאמר זה אצביע על דרך פעולה שתבטיח שימוש הולם בטכנולוגיה למלחמה בטרור. יפורטו עקרונות לבניית מערכת ההגנה תוך מיפוי היכולות הנדרשות לה וכן יוצג הצורך בהרחבת השימוש בטכנולוגיות צבאיות קיימות ובמאמץ לפיתוח יכולות לצרכים שעדיין אין להם מענה בטכנולוגיות הקיימות.

הטכנולוגיה בארגוני הטרור

עקרונית, מבחינים ב**אַסימטריה** בין ארגוני הטרור לבין המדינות המתגוננות מפניהם: המגנים חייבים להתמודד עם איומים רבים ומגוונים בעת ובעונה אחת ונאלצים לפזר את מאמציהם. לעומתם, ארגוני הטרור יכולים להתמקד במספר מצומצם של מטרות ולהבטיח את ההצלחה באתרם את "עקב אכילס" של כל אחת מהן.

לארגוני הטרור אין אמנם את התשתית הטכנולוגית המבוססת והתקציבים לפיתוח מערכות מתקדמות ומתוחכמות, אך אין בכך כדי למנוע מהם לבצע פיגועים מוצלחים בהשתמשם ב**טכנולוגיה פשוטה** — Low Tech. Technology. כך, למשל, אפשר לאיים על התעופה האזרחית בטילי קרקע־אוויר פשוטים (Strela) ולהשתמש בטילי נ"ט אישיים (Law) שאפשר לקנותם בזול בשוק הנשק העולמי.

ברור שלארגוני הטרור יש היכולת להשתמש בכמות קטנה (מספר קילוגרמים) של **חומר נפץ** ובאמצעי הפעלה פרימיטיביים יחסית לביצוע פיגועי התאבדות עם חומר נפץ על הגוף, פיגועי התאבדות במכוניות תופת, מטענים המופעלים מרחוק במבנים או בצד צירי תנועה. עוצמת המופע של פיגועים אלו ועוצמת הנזק והלחץ הנפשי המופעל על האזרחים מעמידים איום זה בעדיפות גבוהה מאד בעיניהם. ירי ב**נשק אוטומטי** על כלי רכב בנסיעה או אל תוך התקהלות, וכן ירי ברובה צלפים על מטרות אנושיות נבחרות הוא איום הנמצא במקום נמוך בהרבה מזה של השימוש בחומרי נפץ.

בנוסף, יש בידי ארגוני הטרור יכולת להפעיל **טרור ממוחשב** – **Cyber Terror** – והטכנולוגיה של התקשורת המתקדמת בעולם, ובכלל זה השימוש באינטרנט, אף היא פתוחה לפניהם. ההסתברות לאירועים מסוג זה עדיין נמוכה, אך משקל האיום אינו נמוך.

ולבסוף, אין להתעלם מן הטרור ה**בלתי קונבנציונלי** ובו אמצעים כימיים, ביולוגיים, רדיולוגיים ואף גרעיניים. צפון קוריאה ואיראן עסקו ועדיין עוסקות בפיתוח אמצעים בלתי קונבנציונליים ובהם טילים לטווח ארוך, וידוע שלסוריה יש ארסנל כימי וביולוגי. גם פקיסטן, שלכאורה נמצאת כיום

בחזית המלחמה בטרור, הודתה בהעברת ידע וטכנולוגיות לפיתוח נשק גרעיני למדינות אחרות. לכל אחת מהמדינות הנזכרות יש עבר עשיר בפעילות חשאית של תמיכה בארגוני טרור ובאספקת מערכות נשק ללא בקרה ופיקוח.

הטרור באמצעים ביולוגיים נתפס כאיום הגבוה בקבוצה זו ומעט מתחתיו מצוי האיום הכימי. האיום בנשק גרעיני, תולדת הפיתוח של ארגון טרור, נתפס נמוך בסולם האיומים משום הסבירות הנמוכה שיכולת כזאת אכן תמומש. סכנה מוחשית יותר היא שאמצעים כאלו יירכשו בידי ארגוני הטרור — מה שקרוי "קיצור דרך" — וכך הם יגיעו ליכולת הפעלה מיָדית.

העקרונות לבניית מערכת ההגנה

חולשתה של המערכת המתגוננת באה לידי ביטוי בהעדר הערכת מצב כוללת של האיום. אין תכנית הגנה הנשענת על זיהוי האיומים, על ניתוח משמעותם ועל קביעת סדר עדיפות בטיפול בהם. בהעדר תכנית כזאת אין יכולת להגדיר צרכים מבצעיים ויכולות נדרשות שיביאו לאיתור טכנולוגיות שכבר קיימות במערכות צבאיות וביטחוניות. אלו הן טכנולוגיות שאפשר להסב לשימוש במערכות הלחימה בטרור בלי מגבלות של ביטחון וסודיות. אם יאומץ סדר עדיפויות חדש, המעמיד את המלחמה בטרור בראש, אפשר יהיה להשתמש במלחמה זו בטכנולוגיות שנשמרו עד כה אך ורק לצורך הפתעה במלחמה הכוללת.

בהעדר תכנית כוללת ובהעדר סדרי עדיפות הנגזרים ממנה, לא ייפלא שהתקציבים המופנים להסבת טכנולוגיות ולפיתוחים חדשים, נמוכים בהרבה מאלו שהיו מקובלים במדינות רבות בעת שהאיום במלחמה כוללת היה על סדר יומן.

המלחמה בטרור מחייבת הכנת **תכנית הגנה** של טיפול באיומים המיָדיים, שאין להם מענה באמצעות היכולות הקיימות, ובו־בזמן היערכות להילחם באיומים העתידיים. האיומים **המידיים** יטופלו בידי יחידות מיוחדות (שחלקן כבר קיימות במדינות כמו ארצות־הברית, צרפת, גרמניה וישראל) ועל ידי שימוש באמצעים הנשענים על יכולות טכנולוגיות קיימות. בתחום זה תהיה תרומה משמעותית ומהירה ליכולת ה"השתלה" של טכנולוגיות קיימות למערכות האמצעים שישתמשו בהם המגנים. איומים **עתידיים** יטופלו באמצעות המערכות שתפותחנה ובאמצעות שיטות פעולה חדשות. התכנית חייבת לכלול הבחנה בסדר העדיפות של הטיפול באיומים, סדר שייקבע לפי חומרת האיום והאפשרויות לגיבוש המענה.

השלב השני הוא **זיהוי טכנולוגיות** הקיימות במערכות צבאיות וביטחוניות ושאפשר להסב אותן, תוך שינויים מזעריים, לצורכי המלחמה בטרור. הכוונה למחושים אופטיים ומכ"מים מתקדמים, מערכות עיבוד נתונים, אמצעי לוחמה אלקטרוניים מתקדמים, מערכות שליטה ובקרה ועוד. חשובות בהקשר זה הן הטכנולוגיות שהיו ממודרות עד כה ומשולבות במערכות נשק שתפקידן לשמש נשק הפתעה להשגת יתרון צבאי במלחמה כוללת. הסבתן, כאמור, תעניק תוספת חשובה לבניית היכולת של מערכות ההגנה מפני טרור.

שלב נוסף הוא ניתוח הפער בין הטכנולוגיות הקיימות, אלו הזמינות לשימוש מידי, לבין הטכנולוגיות הנדרשות כדי להתמודד עם איומים עתידיים. ניתוח זה יישען גם על סדר העדיפות שהוזכר לעיל והוא יאפשר לגבש תכנית כוללת למאמץ המחקר והפיתוח בהתאם לצרכים של המלחמה בטרור.

השלב הרביעי הוא **הפניית תקציבים** מתאימים. מדינות שטרם החלו בפעילות זו תיאלצנה להישען על הישגי המדינות שכבר יצאו לדרך או לגבש תכניות חירום כדי לסגור את הפערים.

השאיפה היא להגיע להפעלת מאמץ מתואם, רב־מדינתי, של מחקר ופיתוח של מערכות הגנה ולחימה. נראה שבעתיד הקרוב יתאפשר להשיק כמה פרויקטים דו־לאומיים. שימוש בטכנולוגיות שאינן רגישות מאוד מבחינה ביטחונית יתרום לקיצור לוח הזמנים בפרק זה של המאמץ. עם זאת, ברור שרק שיתוף פעולה רב־לאומי של מחקר ופיתוח בתחום הטכנולוגיות המתקדמות עשוי להביא ליכולת התמודדות מקיפה.

מיפוי היכולות הנדרשות למלחמה בטרור

ברור שאין יכולת לטפל באיום הטרור באמצעות טכנולוגיה אחת, בידי קבוצת אנשים אחת או על ידי קו הגנה אחד. התפיסה צריכה אפוא להתבסס על "שכבות של הגנה". ברור גם, שאין אפשרות "לחסן" את כל האוכלוסייה בעולם כנגד כל האיומים, ולכן יש להתמקד באיומים המסוכנים ביותר ולמצוא מענה "חיסוני" נגדם. התמקדות כזאת תאפשר לאתר את היכולות הנדרשות למלחמה בטרור וגם לסייע בקביעת הדרכים להשגתן. להלן כמה דוגמאות ליכולות הנדרשות:

הבחנה וזיהוי של בני אדם — יש לסגל יכולות אלו במגוון רחב של מצבים, למשל בשלבי ההתארגנות וההכנות לפעילות טרור,

בשלב של תנועה בין מדינות או בתוך מדינה, בכניסה למקומות ציבוריים, בכניסה לשדות תעופה ובשלבים הקרובים לביצוע הפיגוע.

הבחנה וזיהוי של חומרים – מדובר בחומרים המשמשים למעשי הפיגוע עצמם, בייחוד חומרי נפץ, מתכות וחומרי לוחמה בלתי קונבנציונליים.

יכולת הגנה – כאן נכללות יכולות רבות ובעיקר יכולת להגנה פיזית על בני אדם, אתרים ומתקנים. האתגר בתחום זה הוא היכולת לשלב טכנולוגיית־חומרים עם מערכות מתקדמות לזיהוי האיום ולאיתורו, וכן אמצעים אקטיביים לסיכול האיום המסוים. בהקשר זה יצוין, שהגנה על רשתות התקשורת מפני Cyber Terror מחייבת יכולות טכנולוגיות מיוחדות.

יכולת המודיעין – איתור מוקדים של התארגנות והכנות, מעקב אחר מגוון פעילויות הטרור בעת ביצוען וזיהוי קבוצות או פעילים בודדים השייכים לארגוני הטרור. כאן יבוא לידי ביטוי, כפי שנראה בהמשך, השימוש בטכנולוגיות של המודיעין האלקטרוני והיישום של יכולות לווייני הביון לסוג זה של השגת מודיעין.

הגנה על **תעבורה אווירית** – שימוש באמצעים ביו־מטריים לזיהוי הנוסעים; הכוונה למערכות המבוססות על חיישנים משוכללים לבדיקת הכבודה ולהגנה טובה על תא הטייסים. במכלול נמל התעופה עצמו נזדקק לשכבות של הגנה היקפית ובכללה מניעת השימוש בטילים אישיים נגד מטוסים.

ההגנה על **נתיבי הים** – לשם כך חיוני להרחיב את אזור הביטחון. אמצעי אבטחה יופעלו כבר במרחק אלפי מילים מנמלי היעד, כלומר אפילו טרם העמסתן של המכולות על האונייה. נוסף על שיתוף הפעולה המודיעיני ואימוץ נהלים ותקנות בינלאומיים, יש בתחום הזה מקום לשימוש נרחב בטכנולוגיות חדשות הן בבדיקות שיקוף שכבתיות של המטענים והן בתשלובת מחושים לזיהוי חומרי חבלה ואף חומרי לחימה בלתי קונבנציונליים.[1]

ההגנה ביבשה עוסקת במכלול שונה של איומים – יש אלפי קילומטרים של גבול בתוואים טופוגרפיים שונים, ואין יכולת לסגרם הרמטית. כאן תופעל סריקה של אמצעי התקשורת והיכולת, שאדון בה בהמשך, של מעקב אחר התקשורת של ארגוני הטרור בעזרת האינטרנט.

המצוי – הרחבת השימוש בטכנולוגיות קיימות

רבים ומגוונים הם הנכסים הטכנולוגיים המשולבים במערכות שפותחו עבור הצבאות לאחר מלחמת העולם השנייה. בין הנכסים הללו יש כאלו שאפשר לשלבם באמצעים הנדרשים למלחמה בטרור.

מחושים אלקטרו־אופטיים, מכ"מים, לייזרים, מגלי ריח ואחרים פותחו לאורך עשרות שנים במאה הקודמת והותקנו בראשים של טילים נגד מטוסים, בטילי אוויר־אוויר, בטילים נגד טנקים, במערכות הגנה של מטוסים ובמערכות הגנה של ספינות ושל טנקים. מערכות אלו ורבות אחרות, כמו המחושים אשר בראשו של הטיל "חץ", יודעות לאתר, לזהות את מטרותיהן ולהגיב נגדן במהירות. האתגר שבהסבת יכולות אלו אינו בתכנון דווקא, שיאפשר להבחין באובייקטים בשדה הקרב החדש, אלא בפיתוח וייצור במחירים שאפשר לעמוד בהם.

חומרים ובייחוד חומרים קראמיים (המשמשים למיגון) וחומרים מרוכבים (Composite Materials) נמצאים בשימוש באפודי מגן ובערכות הגנה לכלי רכב ולכלי טיס (מסוקים). האתגר הוא להרחיב את השימוש בחומרים קלים יותר שמשקלם יענה לדרישות. גם בנושא זה האתגר העיקרי הוא לצמצם עלויות.

יכולות זיהוי בעזרת תוכנות היודעות לעבד בו־בזמן פלט של המחושים השונים, קיימות זה כבר במערכות הנשק המתקדמות. "שדה הקרב" של הטרור יחייב במקרה זה מאמץ הסבה גדול יותר כדי להעניק למגנים יכולת לזהות אדם ומערכות המשמשות לפיגוע בטווח ובזמן שיאפשרו למנוע את הנזק או לצמצמו. דרגת חופש מסוימת להתרעות שווא, שהמערכת המגנה תשלים עמה, תאפשר עלויות נמוכות יותר של מערכות ההתרעה ולוח זמנים קצר יותר לפיתוח ולהצטיידות בהן.

מערכות שליטה ובקרה לקרב היבשה נמצאות כיום בשימוש. למערכות אלו יש יכולת לקבל נתונים ממקורות שונים, מן האוויר ומן היבשה, ולתת לכל דרגי הפיקוד תמונת מצב מלאה על האויב ועל כוחותינו בכל רגע נתון. יכולות אלו, במאמץ מזערי של הסבה, תשמשנה למעקב רב־מוקדי אחר פעילות ארגוני הטרור ולתיאום בזמן אמת בין מרכזי פיקוד של מדינות השותפות ללחימה בטרור.

מערכות להגנה נקודתית, למשל הגנה באמצעות מערך טילי קרקע־אוויר או הגנה בעזרת לייזר רב־עוצמה, ישמשו בעיקר להגנת מתקני תשתית ומרכזי שלטון. מערכות אלה יקרות, אך המספר המצומצם של יעדים שיש להגן עליהם עושות אותן לראויות וכדאיות. במסגרת זו נכללת מערכת "נאוטילוס" להגנה נגד רקטות לטווחים קצרים ובינוניים. זו בנויה על חיישני מכ"ם

מתקדמים ועל קרן לייזר רבת־עוצמה והיא נמצאת בשלב מתקדם של פיתוח בצבא ארצות־הברית בשיתוף עם צה"ל.

מערכות מודיעין אלקטרוני — SIGINT, ELINT — שמקצתן כבר "הופשרו" לשימוש נגד הטרור — משולבות בצבאות רבים באופן הדוק בשדה הקרב של המלחמה הכוללת. האתגר של "גיוס" חלק גדול יותר של יכולות אלו למלחמה בטרור הוא בעיקר בהורדת הסיווג הביטחוני מן המערכות שיש להסב.

טכנולוגיות חלל יושמו בעבר, במאבק הבין־גושי, עבור לוויינים ומגוון מחושים בחלל ובמטוסים מגביהי־טוס ללא טייס. מדובר כאן בתפנית בחשיבה, ועל־פיה תופנה יכולת ששירתה בעבר אך ורק צורך אסטרטגי, למעקב אחר פעילות ארגוני הטרור.

הרצוי – צרכים שעבורם יש לפתח יכולות טכנולוגיות חדשות

לצרכים מסוימים אין כיום מענה הולם בטכנולוגיות המצויות ברשותנו. למשל, בתחום חומרי הנפץ יידרשו מחושים בעלי רגישות גבוהה, כדי להבחין בהם מרחוק (100 מטר ואף יותר). זיהוי מוקדם של חומרי הנפץ יחייב, נוסף על טכנולוגיות החישה החדשות, שילוב של שיטות שונות למערכת שלמה המבחינה, מזהה ומאפשרת הפעלה מידית של אמצעי מניעה.

שילוב של יכולת חישה ו"הצלבה" של תוצאות חישה מחיישנים הפועלים על־פי עקרונות פיזיקליים שונים, נדרש גם בתחום המטענים הימיים והיבשתיים. יכולת סריקה של 100 אחוזים של המכולות בזמנים סבירים ובעלויות סבירות, מצריכה מאמץ פיתוח ניכר.

העלויות מכבידות גם על מתן הגנה למטוסי נוסעים. במקרה זה הבעיה אינה בהעדר פתרון ראוי. המטוסים הצבאיים ומטוסים אזרחיים (למשל מטוסים של ראשי מדינה) כבר מצוידים באמצעי הגנה. קפיצת המדרגה הטכנולוגית הנדרשת היא בפיתוח מחושים זולים ושילובם במערכת התרעה במטוס. מערכת זו צריכה לתת הגנה לכל המטוסים האזרחיים במחיר סביר.

הצלבת נתונים ושילוב דיסציפלינות נחוצים גם כדי לפתח מערכת לאיתור הכנות לפעילויות טרור ומעקב אחריהן. כאן תידרש יכולת לזיהוי קולי וחזותי (ממרחק) של בני אדם. על בסיס מאגר ממוחשב של קולות וקלסתרים, שאותו אפשר לבנות בטכנולוגיה קיימת, יש לפתח יכולת הבחנה בתבניות — Pattern Recognition — שתעניק למערכת זו את היעילות והאמינות הנדרשות.

השילוב של הצלבת נתונים עם מחושים רגישים חיוני גם במערכות להבחנה ולזיהוי מהיר של חומרי לחימה ביולוגיים וכימיים. העיקרון של היעזרות במגוון מחושים, כמו במקרה של זיהוי חומרי נפץ, יעניק למערכת אמינות גבוהה ורמה נמוכה של התרעות שווא. בנוסף, תידרש יכולת ניתוח של אותות ותבניות חריגות בתקשורת — Communication Pattern Recognition — לזיהוי ומעקב אחר התקשורת של ארגוני הטרור באינטרנט ובאמצעי התקשורת האחרים.

באילו תחומים יש להתמקד בעתיד הקרוב? כדי להשיג יתרון למגנים במלחמה מיוחדת זו, זקוקה המערכה נגד הטרור להישגים המפורטים להלן ובהקדם האפשרי:

גילוי וזיהוי חומרי נפץ — כאמור, היכולת להבחין מרחוק (100 מטר) בחומר נפץ היא אתגר לא מבוטל. יכולת כזאת חיונית להשגת מגוון פתרונות חדשים ויעילים לאיום שכיום נראה שאין לו מענה. האתגר הוא להגיע ליכולת נְטרול (מרחוק) של מנגנוני ההפעלה של המטענים בעזרת אמצעים המשלבים מחושים שונים המגבים ומשלימים זה את זה. ריבוי המחושים יעניק רמה גבוהה של אמינות לביצועי המערכת.

אמצעי מודיעין — הטכנולוגיה של בסיס הנתונים (Database Technology) עשויה לתרום גם ליכולת הגנתית וגם ליכולת התקפית. בתחום זה נכללים תוכנות ומתודולוגיות הבונות יכולת להגיב לשאילתות ולעדכן דרישות ממסה גדולה של נתונים.[2] יכולת זו תשמש להבחנה אוטומטית של תבניות חריגות בתנועה של אנשי ארגוני הטרור בין מדינות ובתנועות של כספים ברשת הבנקאית הבינלאומית. הטכנולוגיה של מולטי־מדיה, כמו זיהוי קלסתרים או השוואת תדמיות (Image Matching) יוסיפו ממד חשוב ליכולת שליפת הנתונים. טכנולוגיה של שליפת טקסטים היא עוד אמצעי למעקב אוטומטי אחר טקסטים בעלי מבנה חופשי (free texts) לצורכי הצבעה, מיון ובסופו של דבר מציאת "נתיב הנייר" שאותו מותירים ארגוני הטרור במהלך ההכנות לפעולותיהם.[3]

פיתוח מענה לטרור ב**תקשורת המחשבים** – בתחום זה נדרשת הגנה על מתקני תשתיות לאומיים ובהם מערכות תקשורת לאומית, מערכות אנרגיה, מערכת הבנקים ותשתית התחבורה. הדרך לפתח הגנה נאותה נגד האיום הזה תהיה באמצעות הגדרה של המערכות הלאומיות הקריטיות ואיתור נקודות התורפה בהן. הישג ראוי יהיה לפתח מערכות הגנה אמינות בעלות כושר לימוד ושיפור עצמי שתתאמנה את עצמן לשינויים ולהתפתחות האיום. עוד

יכולת חשובה תהיה היכולת לאתר מיד את "מפגע התקשורת" שתאפשר תגובה מהירה ותנטרל את האיום ואת המפגע עצמו.

עד כה "יודע" העולם לעסוק באיום הבלתי קונבנציונלי מול מדינות. עוסקים בכך בסוכנות הבינלאומית לאנרגיה אטומית (סבא"א), באו"ם, באיחוד האירופי ובמספר רב של מוסדות מחקר. לעומת זאת, אין ניסיון ממוקד לרתום את הטכנולוגיה לצורך מעקב ולצורך מניעה של השימוש בטרור בלתי קונבנציונלי בידי הארגונים המאיימים להשתמש בו. אין ספק שאת ה"מקל" של המלחמה בטרור בלתי קונבנציונלי יש לאחוז בשני קצותיו, משמע פיקוח יעיל על המדינות העלולות לספק את החומרים ומאמץ למנוע מן הארגונים הרוכשים להעביר ולהפעיל אמצעים אלו.

מעקב אחר העברה חשאית של חומרים בקיעים או של מתקנים גרעיניים מחייב לפתח מערכות לזיהוי חומרים אלה. מערכות אלה יישענו על טכנולוגיות המנצלות חתימות פיזיקליות מובהקות של החומרים הגרעיניים.

טרור ביולוגי — הנושא נמצא על סדר יומו של המשרד להגנת העורף בארצות־הברית. המשרד יזם פרויקט המכונה "מגן ביולוגי" Project Bio Shield,[4] שאמור להעלות את יכולת ההתגוננות של ארצות־הברית בתחום הטרור הביולוגי למדרגה גבוהה באופן ניכר מזו הקיימת. כיום נדרש מאמץ טכנולוגי, שיניב אמצעים **לגילוי מהיר** של הרכבו של החומר הביולוגי ולהכנת אמצעי חיסון לקראת פיגוע ביולוגי, אך בעיקר אמצעים לטיפול אחרי פיגוע כזה.

סיכום

הטכנולוגיה אמנם אינה האמצעי היחיד במלחמה בטרור — אין להמעיט במשקלם של ההיבטים החברתיים, המשפטיים, הפסיכולוגיים, הכלכליים והפוליטיים — אבל היא תתרום לפעולה יעילה יותר במלחמה זו. אין להמתין עד שתגובש תפיסה כוללת של הגנה, כדי להתחיל בפעילות הטכנולוגית הדרושה להסבת מערכות צבאיות קיימות לצורכי מלחמה בטרור ולפתח מערכות חדשות. כל נושא שאפשר להתקדם בו ולהגיע ליכולת, ולו גם נקודתית, יתרום לחיזוק ההגנה מפני הטרור.

לישראל יש טכנולוגיות בשלות להסבה — טכנולוגיות שאפשר להסיר מהן את האיסורים הביטחוניים — ויכולת פיתוח לצרכים עתידיים, והיא יכולה לשמש דוגמה למיצוי היכולת הטכנולוגית למטרת המאבק בטרור.

הערות

1. הפיגוע הכפול בנמל אשדוד אכן מחדד את הצורך בטיפול מקיף בבעיה של השימוש במכולות. נוסף על נהלים ונוסף על התארגנות לשימוש ביכולות קיימות (ויקרות), צריך לפתח מערכות מתקדמות ולא יקרות כדי להשיג שליטה מרבית בתנועת המכולות בעולם.
2. מדובר ביכולות אחסון וחיפוש בנתוני מולטי־מדיה, כמו תמונות, קולות, דיבור, גרפיקה ווידיאו, וכן שליפת נתונים מתוך מאגרים.
3. השימוש במאגרי נתונים ובמעקב אחר התקשורת האישית מעלה שלושה נושאים הראויים לבחינה ולהסדרה: (א) פגיעה בצנעת הפרט ובזכויות האדם, המעוררת שאלות חוקתיות ומשפטיות הן בתוך המדינות והן במישור הבינלאומי; (ב) הכניסה ל"קודש הקודשים" של הטכנולוגיות הצבאיות, בייחוד למאגרי־הנתונים בתחומי המודיעין, אינה מובנת מאליה עבור כל המדינות אשר מייחסות ליכולת זו חשיבות אסטרטגית ממעלה ראשונה; (ג) התאום בין ארגונים שונים בתוך המדינות ובין ארגונים במישור הבינלאומי, קשה להשגה בגלל מבנים ודפוסי התנהגות הטבועים בהם מטבע בריאתם.
4. בנאומו בכנס הביולוגי, ביוני 2003, המריץ הנשיא בוש את הקונגרס לאשר את החקיקה בנושא הגנה ביולוגית. במסגרת הזאת מתכוון הממשל להשקיע עשרה מיליארד דולר בעשר שנים במחקר ובפיתוח חיסונים יעילים וטיפולים נגד תוצאות הטרור הביולוגי.