הממד החמישי
היערכות ישראל למתקפת סייבר נרחבת

הסייבר הפך לממד הלחימה החמישי, והאיומים הנשקפים ממנו חמורים לא פחות מאשר האיומים שנשקפים לישראל מכל הממדים האחרים. לכן יש להקים בצה"ל פיקוד סייבר

מבוא

באחרונה הגביר צה"ל באופן משמעותי את העיסוק במרחב הקיברנטי[1] מתוך ההבנה שהמרחב הזה מתפתח למרחב לחימה חמישי[2] נוסף על מרחבי הים, היבשה, האוויר והחלל. למרחב הלחימה הקיברנטי יש תכונות ייחודיות המאפשרות לפעול בו במהירות של אלפיות השנייה נגד אויבים המצויים במרחק רב מן המדינה - ובלי לסכן לוחמים. התכונות הייחודיות של המרחב הזה עושות אותו אטרקטיבי ללחימה גם בתקופות שבין מלחמות קונוונציונליות.

מומחים רבים סבורים שהמלחמה הבאה עשויה להתאפיין בתקיפות קיברנטיות מתואמות המיועדות לעצב את מרחב הלחימה הרחב יותר ולהשפיע על קשת רחבה של כוחות ושל מוקדים אסטרטגיים. בראשית המאה ה־21, שבה כל העולם תלוי באינטרנט, עשויה העליונות במרחב הקיברנטי להיות מכריעה כפי שהייתה השליטה באוויר במשך רוב המאה ה־20.

מדינות מודרניות וצבאות מתקדמים בעולם - ובהם ישראל וצה"ל - מגבירים את פעילותם במרחב הקיברנטי שהוא בעבורם מקור עוצמה, אך גם חושף "בטן רכה".[3] באחרונה אף הודיעה ארה"ב שהיא רואה בתקיפת תשתיות מקוונות עילה למהלכים מלחמתיים.[4] באחד מנאומיו האשים נשיא ארה"ב ברק אובמה לראשונה באופן מפורש את ממשלת סין בגל התקיפות האחרון על אתרים של חברות אמריקניות ועל תשתיות במדינה.[5]

אשר לישראל - טכנולוגיות המידע והמרחב הקיברנטי תורמים תרומה מכרעת ליתרון האיכותי של ישראל בתחומי הביטחון והכלכלה. המרחב הקיברנטי חיוני לחברה, לקשר בין הממשל לאזרחים ולקשרי ישראל עם העולם. ואף יותר מכך, למרחב הזה יש חשיבות רבה לביטחון הלאומי של ישראל בהתחשב באיומים הקיברנטיים המתהווים, ביתרונה של ישראל בתחומים של טכנולוגיות המידע ובפוטנציאל שיש למרחב הקיברנטי בשדה הקרב המודרני.

בשנים האחרונות עוסק צה"ל בהטמעת מערכות טכנולוגיות רבות. תוכנית "צה"ל ברשת",[6] שעליה הכריז ראש אגף התקשוב לפני כעשור, הפכה את צה"ל לצבא מודרני יותר המבוסס על טכנולוגיה ועל יכולות תקשורתיות מתקדמות. במסגרת היערכות צה"ל לשינוי המתהווה ומתוך ראייה מערכתית כוללת הוקמה מחלקת הגנות בסייבר.[7]

על הפרק עומדות כעת כמה שאלות יסוד ובהן כיצד מגינים על הנכסים הקיברנטיים של המדינה ומהו מקומו של צה"ל בהתארגנות הזאת. בשאלות האלה מתמקד המאמר הזה. כדי ליצור שפה משותפת יש קודם כול להגדיר

ראש הממשלה בנימין נתניהו מכריז על הקמתו של מטה הסייבר בראשות פרופ' יצחק בן ישראל (מימין), מאי 2011 | ראש הממשלה דרש שאיום הסייבר הוא אחד מחמשת האיומים המרכזיים על הביטחון הלאומי של ישראל

אל"ם נתי כהן
רמ"ח תכנון באגף התקשוב,
בוגר מב"ל

כמה מושגי יסוד ולהציג כמה נקודות מוצא בתחום הזה.

התקפה קיברנטית

התקפה קיברנטית היא לחימה במרחב הקיברנטי נגד אויב כדי לגרום לו נזק: לפגוע בתפקודו ולגרום לו לנהוג לפי רצון התוקף. התקפה קיברנטית בפני עצמה אינה מסוגלת להביא להכרעה[8] או להביא הישגים אסטרטגיים כמו כיבוש שטחים על ידי צבא יבשה, אך היא מסוגלת לפגוע ביעדים חיוניים של האויב וביכולותיו.[9] יש להניח שהתקפה קיברנטית עשויה להיות רכיב בכל מלחמה מודרנית בעתיד - לצד מרכיבי כוח אחרים. התכונות הייחודיות של המרחב הקיברנטי עושות אותו אטרקטיבי ללחימה גם בתקופות שבין מלחמות קונוונציונליות. התקפות קיברנטיות עשויות לשמש לתכליות האלה:

1. אמצעי להפעלת לחצים לשינוי מדיניות היריב בתקופות שבין מלחמות קונוונציונליות.
2. סיכול איומים ביטחוניים מתהווים, כמו התקיפות באמצעות התולעת סטוקסנט (Stuxnet) באיראן.
3. בניית יכולות התקפה במסגרת בנייתו של מאזן הרתעה.
4. תגובת־נגד - פגיעה קיברנטית בתוקפים או במדינות שמהן יוצאות התקפות קיברנטיות.[10]

הגנה במרחב הקיברנטי

מסמך של צבא ארה"ב מ־2010, שאת רובו אימצו צה"ל ומטה הסייבר הלאומי, מגדיר כך את המושג "הגנה קיברנטית" (Cyber defense) ברמה האופרטיבית: "מכלול פעולות המשלבות הגנה על רשתות מחשב והגנה על תשתית קריטית לכדי מערכה רחבה, שממנה אפשר גם להגיב במתקפת נגד או במתקפת מנע. במסגרת ההגנה במרחב הקיברנטי נוקטים, בין היתר, מגוון רחב של צעדים שמטרתם למנוע פגיעה ולהפחית סיכון ונזק לתשתיות של תקשורת מחשבים המוגדרות חיוניות. בכך נכללות גם פעולות כגון: יתירות (יכולות עודפות וגיבויים), בידוד מערכות מידע מסוימות, בידול בין מערכות, פריסת מערך אבטחת מידע קונוונציונלי בכמה שכבות, אבטחה פיזית של מערכות המידע ונוהלי ביטחון מידע נוקשים ומשתנים ותרבות המשתמשים".[11]

> התקפה קיברנטית היא לחימה במרחב הקיברנטי נגד אויב כדי לגרום לו נזק: לפגוע בתפקודו ולגרום לו לנהוג לפי רצון התוקף

איסוף קיברנטי

איסוף קיברנטי (Cyber Network Exploitation) הוא איסוף מידע באמצעות ניצול של רשתות המחשבים בשילוב עם יכולות מסייעות (כמו תמיכה בלוחמה אלקטרונית ובמודיעין אותות) למטרות מודיעין ומאמצים אחרים. הרחבת המושג "איסוף קיברנטי" לתחום ההגנה משמעותה היכולת לאסוף מידע לצורך סיכול התקפה במרחב הקיברנטי.

טרור קיברנטי

טרור קיברנטי הוא פעולת טרור הנעשית במרחב הקיברנטי או באמצעותו. כבר היום, אפשר לראות שארגוני טרור מהג'יהאד העולמי עושים שימוש רב - אם כי מוגבל ועדיין לא מפותח יחסית - במרחב הקיברנטי כדי לממש את יתרונותיו בעבורם. אלה השימושים העיקריים שעושים ארגוני הג'יהאד העולמי בתחום הקיברנטי:

- **תעמולה** - הפצת רעיונות, פסיקות, הנחיות, נאומים ודעות של אנשי דת ושל מנהיגי טרור.
- **גיוס ואימון** - איתור חברים פוטנציאליים וגיוסם וכן העברת חומרי הדרכה באמצעות הרשת.
- **גיוס כספים ומימון** - באמצעות התחזות לארגוני צדקה וסיוע ובאמצעות גניבת זהויות וכרטיסי אשראי.
- **תקשורת** - ניצול הרשת לתקשורת מבצעית באמצעות שימוש בכלי הצפנה זמינים.
- **איתור מטרות ומודיעין** - באמצעות הפקת מידע מהרשת.[12]

נכון לעת הזאת טרם נודע על תקיפה קיברנטית של גורמי טרור, ולכן האיום הזה אינו נראה מיידי.

המאפיינים של זירת הלחימה הקיברנטית

המרחב הקיברנטי הופך בהדרגה לממד חדש בלחימה - ממד שיש לו מאפיינים ייחודיים ושונים מהמקובל בעולם הצבאי. מדינות וארגונים חסרי משאבים מדיניים לצד מעצמות צוברים יכולות וניסיון התקפיים, כך שלמעשה נוצרים איומים אסימטריים על ישראל שקיומה תלוי במידה רבה בפעילות במרחב הקיברנטי.

אפשר לעמוד על המשמעות של הקמת הממסדים הביטחוניים הקיברנטיים באמצעות אנלוגיה בין התפתחות הלוחמה במרחב הקיברנטי לבין התפתחות הלוחמה במרחב האווירי.

המרחב האווירי קיבל את חשיבותו האסטרטגית במהלך המחצית הראשונה של המאה ה־20, לאחר שהתברר כי הוא מאפשר פעולות צבאיות מסוג חדש - היישר נגד הבטן הרכה של האויב, במהירות ובלי להתכתש עם כוחות היבשה שלו. באנלוגיה למרחב האווירי, הרי מבחינת הקמת הממסדים מצוי כיום המרחב הקיברנטי במקום שבו היה הכוח האווירי בשלהי מלחמת העולם הראשונה. הקמת ממסדים ביטחוניים קיברנטיים עשויה לחולל מהפכה דומה בחשיבה ובעשייה הצבאיות. במרחב הקיברנטי קיים פוטנציאל להתפתחות מהירה יותר מזו שהייתה במרחב האווירי, אך מימושו תלוי במוטיווציה הפוליטית המושפעת, בין היתר, מאירועים ביטחוניים.[13]

תפיסת הסייבר בצה"ל

על פי תפיסת הסייבר בצה"ל, המרחב הקיברנטי הוא ממד לחימה ייחודי שבו ניתן לנהל מבצעים ופעולות של איסוף, של תקיפה (אסטרטגית, מערכתית וטקטית), של שלילת יכולות ושל הגנה כדי לשמר ולהבטיח את רציפות הפעולה המבצעית של צה"ל במסגרת רעיון מבצעי כולל.

אירועי פגיעה במרחב הקיברנטי

רשימת אירועי התקיפה המיוחסים למדינות היא קצרה ודלה. יתר על כן, אף על

פי שבמדינות המערב קיימת ציפייה דרוכה לטרור קיברנטי, עד כה לא ידוע על תקיפה קיברנטית משמעותית שעשה ארגון טרור, ושום מדינה או ארגון טרור לא קיבלו אחריות לתקיפה קיברנטית.

אוגוסט 2008 - מלחמת רוסיה-גאורגיה על דרום אוסטיה

בתחילת אוגוסט 2008 פלשה גאורגיה לדרום־אוסטיה כדי להחזיר לעצמה את השליטה בחבל שהיה בעבר שלה, אך פרש והכריז על עצמאות. רוסיה מיהרה להתערב בלחימה, הביסה בתוך זמן קצר את צבא גאורגיה ושמרה על עצמאותה של דרום־אוסטיה.[14]

במהלך העימות בין רוסיה לגאורגיה היו מתקפות קשות על אתרים ועל שרתים של הממשל בגאורגיה. הפעולות האלה לא גרמו לנזק פיזי של ממש אולם הן החלישו את הממשל הגאורגי בזמן הקונפליקט. בין היתר הן פגעו ביכולתו לתקשר עם הציבור במדינה ועם דעת הקהל בעולם.[15]

המתקפה הקיברנטית על גאורגיה לא עמדה בפני עצמה אלא קדמה לפלישה של כוחות יבשה רוסיים למדינה. נראה שתכליתה הייתה לפגוע בקשר בין הממשל לאזרחים. המקרה הזה הוא דוגמה ללוחמה קיברנטית שנועדה לסייע למאמץ הצבאי הכולל.[16]

ספטמבר 2010 - מתקפת סטוקסנט על איראן

מתקפת הסטוקסנט נגד איראן מסמנת עידן חדש בלוחמה במרחב הקיברנטי. בספטמבר 2010 נודע שמתקני גרעין באיראן נפגעו מתולעת שכינויה היה סטוקסנט. חברת האבטחה העולמית סימנטק, שפירסמה דו"ח מקיף בנושא,[17] העריכה שהתולעת נועדה לפגוע בפעולת הצנטריפוגות להעשרת אורניום שהחלו לפעול באיראן מ־2007.[18]

מאוחר יותר אישרה אירן שמערכת המחשוב במתקניה הגרעיניים נפגעה מווירוס הרסני. כמן כן הודתה כי גם המחשבים האישיים של בכירים בתוכנית הגרעין נפגעו במתקפה. סוכנות הידיעות הרשמית של איראן דיווחה כי בין המחשבים שנפגעו היה גם מחשבו של מחמוד ג'אפרי, מנהל הכור הגרעיני בבושהר. לדברי מנהל ההגנה האזרחית של איראן, ראזה ג'לאלי, שצוטט בסוכנות הידיעות האיראנית, חקירת התקיפה הממוחשבת העלתה כי התוכנה נוצרה בישראל ובטקסס שבארה"ב.[19]

האירוע עורר בעולם שיח בנושא הלוחמה במרחב הקיברנטי. קהילות האבטחה במרחב הקיברנטי רואות בתקיפת סטוקסנט אירוע מכונן. קיימת תמימות דעים שהתקיפה עשויה לסמן קפיצת מדרגה הן בתחום ההגנה והן בתחום של פיתוח נשק להתקפה. המשמעות העיקרית שמייחסים מומחים בעולם לאירוע היא שתקיפת סטוקסנט שונה מהתקיפות הקודמות, משום שזו תקיפה בכלי מתוחכם לאין שיעור הממוקד ביעד ביטחוני מסוים, להבדיל מתקיפות קודמות, המיוחסות בעיקר לרוסיה, שנעשו בכלים פרימיטיביים ובחזית רחבה.[20]

תקיפות המיוחסות לסין - חשיפת יחידה 61398

בשנים האחרונות נערכו תקיפות על תשתיות שהיו בבחינת קפיצת מדרגה. הראשונה הייתה סדרת התקיפות Shady RAT שהחלו באמצע 2006 ונמשכו עד פברואר 2011. סדרת התקיפות השנייה הייתה מבצע Aurora שהיה מתוחכם במיוחד ובו הותקפה, בין היתר, חברת גוגל שהיא כיום תשתית חיונית כלל־עולמית. התקיפות האלה נערכו מאמצע 2009 ועד דצמבר של אותה השנה. סדרת התקיפות השלישית - שלה היו הדים רבים בתקשורת - הייתה נגד חברת RSA שמאבטחת מידע ושרתי אינטרנט ומספקת, בין היתר, שירותי SecureID (כניסה מאובטחת למחשבים באמצעות שילוב של כרטיס חכם ושל סיסמה) והרשאות כניסה חד־פעמיות. ההנחה הרווחת היא ששין עמדה מאחורי התקיפות האלה.[21]

נשיא ארה"ב ברק אובמה פנה למקבילו הסיני בתחילת מרס 2013 והעלה חשש מפני הידרדרות חמורה ביחסים בין שתי המדינות בשל הפריצות המרובות לשרתים של חברות הטכנולוגיה הגדולות בארה"ב, ובהן פייסבוק, גוגל, אפל מיקרוסופט וטוויטר. זו הייתה הפעם הראשונה שבה נשיא אמריקני מאשים באופן ישיר את המשטר בסין באחריות לתקיפות הסייבר.

ארה"ב כבר הודיעה שהיא רואה בתקיפה מקוונת של תשתיות עילה למהלכים מלחמתיים, וגורמים בוושינגטון אף המליצו לשקול תקיפה גרעינית בתגובה לגרימת נזק

נשיא ארה"ב ברק אובמה בפגישה עם נשיא סין שי ג'ינפינג, קליפורניה יוני 2013 | באחרונה הודיעה ארה"ב שהיא רואה בתקיפת תשתיות מקוונות עילה למהלכים מלחמתיים. באחד מנאומיו האשים אובמה לראשונה באופן מפורש את ממשלת סין בגל התקיפות האחרון על אתרים של חברות אמריקניות ועל תשתיות במדינה

כוחות רוסיים בדרום־אוסטיה, 2008 | במהלך העימות בין רוסיה לגאורגיה היו מתקפות קשות על אתרים ועל שרתים של הממשל בגאורגיה. הפעולות האלה לא גרמו לנזק פיזי של ממש, אולם הן החלישו את הממשל הגאורגי בזמן הקונפליקט. בין היתר הן פגעו ביכולתו לתקשר עם הציבור במדינה ועם דעת הקהל בעולם

נרחב לתשתיות. עם זאת, הנשיא סייג את דבריו והסביר כי יש להימנע מ"רטוריקה מלחמתית". הוא קרא לקונגרס לפעול לחיזוק מערך ההגנה מפני התקפות האקרים בלי לפגוע בחופש הגלישה של אזרחי המדינה.[22]

ה"ניו־יורק טיימס" דיווח שהמודיעין האמריקני גילה את המקום שממנו מנהלת סין את המלחמה המקוונת נגד ארה"ב: בניין בן 12 קומות השוכן בפרבר של שנחאי. על פי הדיווח, על מבצעי הפריצה למחשבים האמריקניים מופקדת יחידה 61398 של צבא סין. חברת מנדיאנט האמריקנית לאבטחת מחשבים פירסמה דו"ח בן 60 עמודים על מתקפות הסייבר הסיניות. בדו"ח מצוינים - בפעם הראשונה - שמות של אנשים מכ־20 קבוצות האקרים מתוחכמות ביותר, ובהן "צוות תגובות" ו"קבוצת שנחאי", שמקושרות ישירות לרב קומות שבו ממוקמת יחידת ההאקרים הלאומית של סין ושממנו נעשות מדי יום התקפות על מחשבים בשטח ארה"ב.[23]

צפון־קוריאה - ניסוי גרעיני ותגובה לסנקציות של מועצת הביטחון

סוכנויות הידיעות דיווחו ב־20 במרס 2013 כי מערכות המחשבים של שלוש רשתות טלוויזיה ושל שני בנקים גדולים בדרום־קוריאה הופלו במה שנראה היה כמו מתקפה מכוונת. צבא דרום־קוריאה הגביר את כוננותו מחשש שצפון־קוריאה עמדה מאחורי המעשה. בין היתר הועלתה הסברה שמדובר בתגובה של צפון־קוריאה לסבב הסנקציות החריף שהטילה עליה מועצת הביטחון בעקבות ניסוי גרעיני שלישי שהיא עשתה בתחילת 2013. פיונגיאנג איימה בתגובה חריפה נגד דרום־קוריאה ונגד ארה"ב ואף איימה ב"מתקפת מנע גרעינית". סוכנות הידיעות הצפון־קוריאנית דיווחה כי מנהיגה, קים ג'ונג און, אמר כי "צפון־קוריאה תהרוס את אויביה ללא רחמים עד שלא יישאר אדם אחד שיחתום על הסכמי הכניעה". צפון־קוריאה אף טענה שארה"ב ודרום־קוריאה עורכות התקפות סייבר נגדה.[24]

אנונימוס מתקיף יעדים ישראליים - 7 באפריל 2013

בין 6 ל־8 באפריל 2013 תקפו עשרות קבוצות - ובהן קבוצות הקשורות לארגון אנונימוס - אתרים בישראל. סיסמת הפעולה שלהם הייתה: "מוחקים את ישראל מהאינטרנט". לתקיפה היה מאפיין אחד בולט: השתתפו בו גורמים רבים שחברו יחד לשם התקיפה. הם החליפו ביניהם מידע וריכזו כוח תקיפה רב למועד מסוים וכיוונו אותו לעבר נקודות חולשה. להלן סיכום קצר של תוצאות התקיפה:

- כל אתרי האינטרנט הממשלתיים וכל השירותים המקוונים המתארחים בחוות השרתים הממשלתית ביחידת ממשל זמין נותרו זמינים לציבור במשך כל ימי ההתקפה. התוקפים לא הצליחו לשבש את אתרי האינטרנט הממשלתיים או לגרום להם נזק.
- שלושה אתרים שאינם מתארחים בחווה הממשלתית נפרצו ועברו השחתה (Defacement): האתר של מכון וולקני, האתר של הקרן לשיקום מחצבות והאתר של נציגות ישראל בבוסטון. בפריצה לאתר של נציגות ישראל בבוסטון נגנב מידע אישי של אזרחים ישראלים ופורסם באינטרנט.
- במהלך המתקפה נפרצו והושחתו מאות אתרי אינטרנט ישראליים - בעיקר אתרים של עסקים קטנים. כמו כן נפרצו אלפי חשבונות פייסבוק של אזרחים ישראלים ובהם גם דף הפייסבוק שמפעיל משרד ראש הממשלה.[25]

מספר התוקפים הוא למעשה מספר כתובות ה־IP שמהן נעשו תקיפות שיטתיות של אתרים ישראליים. מספר המדינות מייצג את מספר המקורות השונים של כתובות ה־IP. עם זאת, לא ניתן לדעת בוודאות את מקור התקיפות כיוון שתוקף יכול לעשות שימוש בכתובת IP ממדינה אחרת או מכמה מדינות שונות.

מסקנות מאירועי התקיפה שנסקרו

מתוך האירועים שנידונו לעיל נראה שלפנינו סוג חדש של מבצעים צבאיים שאפשר לכנותו "מבצעי מידע ותשתית".[26] למבצעים האלה כמה מאפיינים בולטים:

1. הם יכולים להשתלב עם סוגי מבצעים אחרים - כפי שהיה, למשל, במלחמת רוסיה-גאורגיה.
2. הם מתנהלים ברובם במרחב הקיברנטי ועשויים לכלול מבצעים מיוחדים ומאמצים קיברנטיים מוגבלים נגד מטרות מפתח בתשתית, נגד נקודות תורפה של יחידות ונגד צווארי בקבוק - כמו, למשל, ההתקפה על אסטוניה ופעולת הסטוקסנט.
3. ניתן לנסות להשיג באמצעותם יעדים אסטרטגיים, מערכתיים וטקטיים.

4. הם מאפשרים להשיג יתרונות חשובים נגד חברות או נגד צבאות התלויים במערכות מרושתות וביכולות מרושתות. זה, למשל, מה שסין מנסה להשיג באמצעות לוחמת הסייבר שהיא מנהלת נגד ארה"ב.
5. הם עשויים להיות גורם מכריע בהשגת מטרות המלחמה.
6. הם יכולים לשמש, למשל, את מי שמנהלים את המאמצים להביא לדה־לגיטימציה של ישראל.

בראש סדר העדיפויות של המטה הקיברנטי הלאומי - מיום הקמתו - נמצא גיבושה של תפיסת הגנה לאומית

המרחב הקיברנטי במדינת ישראל - תמונת מצב

החלטות שהתקבלו ויישומן עד כה

ישראל הייתה מהמדינות הראשונות בעולם שהכירו בחשיבות ההגנה על מערכות ממוחשבות חיוניות. במהלך 1997 הוקם פרויקט תהי"ל (תשתית הממשלה לעידן האינטרנט) שמטרתו הייתה להגן על החיבור של משרדי הממשלה לאינטרנט ולספק למשרדי הממשלה שירותי גלישה מאובטחים. בתהי"ל הוקם "מרכז אבטחת המידע של ממשלת ישראל".

החלטת הממשלה על "קידום היכולת הלאומית במרחב הקיברנטי"

המטה הקיברנטי הלאומי הוקם בינואר 2012, ובראשו עומד ד"ר אביתר מתניה. המטה - בשילוב עם הגופים הרלוונטיים - אחראי לגיבושה של מדיניות הגנה כוללת למרחב הקיברנטי ולבנייתם של תפיסת הגנה לאומית ושל שיתופי פעולה.

בראש סדר העדיפויות של המטה הקיברנטי הלאומי - מיום הקמתו - נמצא גיבושה של תפיסת הגנה לאומית. אלה הם הגופים המופקדים כיום על היערכות המדינה להגנה בפני מתקפת סייבר:

1. **מטה הסייבר הלאומי.** זהו גוף מטה שכפוף לראש הממשלה, ממליץ על מדיניות קיברנטית לאומית ומקדם את יישומה.
2. **הרשות הממלכתית לאבטחת מידע (רא"ם).** זו מופקדת על הנחיה מקצועית של הגופים שבאחריותה בתחום של אבטחת תשתיות מחשב חיוניות מפני איומי טרור וחבלה ובתחום של אבטחת מידע מסווג מפני ריגול וחשיפה.[28]
3. **אגף התקשוב הממשלתי, ובתוכו תהי"ה.** זהו הגוף המרכזי שמספק שירותי גלישה מאובטחים למשרדי הממשלה ולמוסדותיה השונים ועושה ככל יכולתו כדי להגן על הרשתות הממשלתיות בחיבור לאינטרנט.
4. **מטה הסייבר בצה"ל.** ההגנה על הסייבר לכלל מערכות צה"ל היא באחריות אגף התקשוב. עם זאת, מטה הסייבר בצה"ל כפוף פורמלית לסגן הרמטכ"ל ומנוהל באופן מעשי ביחידה 8200 של אגף המודיעין. לפי ההגדרות של צה"ל, הלחימה בסייבר היא זירת הלחימה החמישית של הצבא לצד הים, היבשה, האוויר והחלל. מטה הסייבר שהקים צה"ל הוא גוף מטה ייעודי לנושא שמשלב בין גורמים באגף המודיעין לאנשי אגף התקשוב שעוסקים בהגנה מפני התקפות סייבר.[29]
5. **היחידה למניעת פשיעה בסייבר במשטרה.** בכוונת המשטרה להקים יחידה חדשה שתעסוק בפשיעה במרחב הסייבר. בהרצאה שנשא המפכ"ל בפני חניכי מב"ל הוא ציין שהקמת היחידה היא יעד מרכזי של המשטרה.
6. **המלמ"ב (הממונה על הביטחון במערכת הביטחון)** אחראי לאבטחה הפיזית של המתקנים הביטחוניים בישראל ולאיתור הפרצות שמהן עלול לזלוג מידע סודי.
7. **הרשות למשפט, לטכנולוגיה ולמידע (רמו"ט)** עוסקת בהגנה על המידע האישי של אזרחי ישראל במרחב הקיברנטי.

נתונים נבחרים על התקיפות הקיברנטיות נגד אתרי ממשלה באפריל 2013[26]

שם האתר	מספר התוקפים	מספר המדינות שמהן באו התוקפים	סך ה"כ התקפות
משרד החוץ	2,028	103	418,437
gov.il	913	70	44,919
בנק ישראל	1,175	57	29,923
משטרה	1,284	60	25,127
gov.il מייל	20,052	2	20,304
משרד המשפטים	1,620	57	18,780
בית הנשיא	909	69	17,860
שב"כ	1,306	85	16,729
דו"צ	331	42	13,337

הוספת המרחב הקיברנטי למרחבי הלחימה המסורתיים (יבשה, ים, אוויר וחלל) מחייבת לשלב אותו בתפיסת הביטחון של ישראל

הוספת המרחב הקיברנטי למרחבי הלחימה המסורתיים (יבשה, ים, אוויר וחלל) מחייבת לשלב אותו בתפיסת הביטחון של ישראל. אולם בחינה של המושגים הרלוונטיים בתפיסת הביטחון של ישראל מלמדת שאלה אינם מתאימים למרחב הלחימה הקיברנטי. למשל, קשה מאוד ליישם את עקרון ההרתעה במרחב הקיברנטי, להתרעה האופרטיבית אין משמעות ללא הגנה אקטיבית, והגנה קיברנטית מחייבת התאמה עמוקה לתכונות הייחודיות של המרחב. יתר על כן, שיתוף הפעולה הנדרש להגנת המרחב הוא חסר תקדים בהשוואה לשיתופי הפעולה האחרים בין הסקטור הביטחוני לסקטור האזרחי לצורך פעילות צבאית. זאת ועוד, לאור ההכרה שהמרחב הקיברנטי הוא מרחב לחימה נפרד יש לבחון יכולות אסטרטגיות חדשות ואולי

אף לחולל שינוי בסדר הכוחות, דהיינו להשקיע יותר בהקמת צבא קיברנטי.

במדינות מערביות רבות הולכת ומתגבשת תפיסת ההגנה שבבסיסה מונחים כמה עקרונות בסיסיים:

1. יש לעבור מאבטחה להגנה, דהיינו יש לאמץ את הגישה שלפיה לא המידע הוא מושא התקיפה, אלא הרשת כולה.
2. על המענה להיות רחב ולהקיף את כל המדינה.
3. אין להפריד בין יעדים ביטחוניים ליעדים אזרחיים.
4. יש לאמץ מענה רחב וגמיש לקראת האפשרות שהאיום יחריף בעתיד.

המטה הקיברנטי הלאומי של ישראל שוקד בימים אלה על גיבושה של תפיסת הגנה קיברנטית למדינה שתכלול עם השלמתה שתי שכבות פעולה:

1. **שכבת האבטחה הארגונית.** האחריות לאבטחה הקיברנטית היא בראש ובראשונה של הארגונים ושל הפרטים - החל מהאזרחים הפרטיים והעסקים הקטנים וכלה בחברות הגדולות, מוסדות המדינה, התשתיות הקריטיות וגופי הביטחון. הכלים והיכולות להתמודד עם האיומים מצויים ברובם ברמה הארגונית.
2. **שכבת הפעולה המדינתית.** הנדבך הזה של ההגנה מיועד לחזק באופן משמעותי את כל הפעולות לאבטחת המידע, המערכות הממוחשבות והרשתות בכל המרחבים הארגוניים והפרטיים.

כדי לממש את תפיסת ההגנה הקיברנטית ברמה המדינתית יש לגבש מתווה ארגוני יעיל שיאפשר סינרגיה בין שכבות ההגנה. אם יוקם גוף הגנה לאומי ייעודי הוא יהיה ציר מקשר בין שכבות ההגנה ויהיה אחראי לגיבושה של תמונת המצב ולניהול אירועים ומשברים ברמה הלאומית.

הסכנה:
תקיפת סייבר נרחבת על ישראל

בנאום שנשא ראש הממשלה נתניהו ב־25 ביולי 2012 בפני חניכי מב"ל בטקס סיום מחזור ל"ט הוא אמר, בין היתר:

הביטחון הלאומי שלנו בשנים אלה יעמוד בפני חמישה אתגרים: "האתגר הראשון הוא הגרעין האיראני, האתגר השני הוא האיום הטילי והרקטי, האתגר השלישי הוא הסייבר, האתגר הרביעי הוא ההגנה על גבולותינו מפני פריצתם והאתגר החמישי הוא מאגרי הנשק שהולכים ונערמים באזורנו".

ישראל מעולם לא הגדירה "איום ייחוס" בתחום הסייבר, דהיינו לא הגדירה מיהם אויביה בתחום הזה, וגם אין בכך צורך. על ישראל להיות ערוכה לאיומים מכל מקור שהוא מהסוג שנשקף ממדינות כמו סין, איראן ורוסיה. ויש לזכור שגם לארגוני הטרור יש פוטנציאל להפוך לסכנה של ממש בתחום הזה. החוכמה היא להימנע מלהיות הצד הנפגע באירועים כאלה באמצעות זיהוי מראש של אזורי החולשות ובאמצעות מודעות לסכנות. את המשימה הביטחונית לסכל התקפה נרחבת בסייבר ניתן להשיג באמצעות נקיטת הפעולות הבאות:

1. תמיכת המדינה ברציפות התפקודית של הגופים התלויים במרחב הקיברנטי.
2. מערך הגנה המבוסס על אמצעים לגילוי ולזיהוי של תקיפות סייבר ועל מידע מודיעיני מקדים.
3. נטרול האיומים לביטחון הלאומי באמצעות שימוש בכל היכולות הקיימות במדינה בתחום של לוחמת הסייבר.
4. מבנה ארגוני תומך.

היערכות ישראל להגנה במרחב הסייבר

המודל שמוצג בפרק הזה מבוסס על שילוב של כל מאמצי ההגנה בתחום הסייבר למערך לאומי אחד אזרחי־צבאי. זאת מתוך ההבנה שמרחב הסייבר אינו מוגבל לארגון מסוים.

הגנה מרחבית ותחומי אחריות

קודם לניתוח המענה הראוי יש למפות את מרחבי הסייבר בישראל בהתאם לכושר ההגנה מפני תקיפות סייבר. לפי הקריטריון הזה ניתן לחלק את ישראל לשלוש קבוצות:

1. **מרחב ההגנה על התשתיות האזרחיות הקריטיות.** המרחב הזה כולל גופים ומוסדות שנקבעים על ידי ועדת היגוי מיוחדת של המטה הקיברנטי הלאומי על פי קריטריונים מוגדרים. למרחב הזה אחראי שירות הביטחון הכללי באמצעות הרשות הממלכתית לאבטחת מידע (רא"ם).
2. **מרחבי ההגנה למערכת הביטחון ולגופים מיוחדים.** לצה"ל, לשב"כ, למוסד, למשטרה, למוסדות ביטחון מיוחדים ולתעשייה הביטחונית יש מערכות משלהם, שלרוב סגורות ברשתות ייחודיות ובמערכי אבטחה ייחודיים. כל אחד מהגופים האלה אחראי למרחב שלו.
3. **מרחב הגנה אזרחי.** המרחב הזה מחולק לשני תת־מרחבים: הראשון הוא המרכז הממשלתי (gov.) שעליו מגן אגף התקשוב הממשלתי, ובתוכו תהיל"ה. השני הוא המגזר האזרחי (על מגזריו השונים: בנקאות, חברות התקשורת, הביטוח וכל מי שלא נכלל בהגנת רא"ם). למרחב האזרחי בסייבר יש להקים "רשות אזרחית להגנה בסייבר" שתהיה כפופה ישירות למטה הקיברנטי הלאומי ושתטפל בהסדרתו של מנגנון ההגנה ושל אמצעי האבטחה.

הגנה חוצת מרחבים

המרכיב השני בתפיסת ההיערכות הכוללת מתייחס לתחום שחוצה מרחבים:

1. **מניעה, חקירה ואכיפה נגד פשיעה במרחב הקיברנטי.** משטרת ישראל היא שממונה על הלחימה בפשיעה במרחב הקיברנטי, אך הגבולות בין פשעים לבין טרור ולבין ריגול - ביטחוני ותעשייתי - הם מטושטשים מאוד, וקיים חשש שגורמי פשיעה יהיו מעורבים בפעילות עוינת בשירות מדינות אויב. לכן בפועל משתתפת המשטרה במאמץ האבטחה הלאומי הכולל בסייבר, ואילו גורמי האבטחה הביטחוניים מוצאים את עצמם עוסקים גם בלחימה נגד פשיעה פלילית בסייבר.
2. **איסוף מודיעין להתרעה ולסיכול תקיפות.** במשימה הזאת עוסקים כיום שלושה גופים מרכזיים הפועלים בהתאם ליתרונותיהם היחסיים: אמ"ן, שב"כ והמוסד. לנטרול איומים המסכנים את הביטחון הלאומי יש להפעיל את כלל היכולות שקיימות במדינה. המשימה הזאת היא נדבך נוסף - אקטיבי יותר - במאמץ ההתגוננות מפני התקפות סייבר. מאחר שהיא מחייבת יכולות רבות, מוצע להטילה על גופי הביטחון - בהתאם לחלוקת האחריות המסורתית ביניהם. עם זאת, עליהם לעבוד בסנכרון ביניהם ובתיאום

←

המבנה המומלץ להיערכות ישראל במרחב הקיברנטי

מערכתי. במסגרת ההיערכות לפעילות הזאת יש להקים מחלקה ייעודית במטה הקיברנטי הלאומי שתעסוק במחקר ובהתרעה מפני מערכי אויב וכן בהכוונה ובתיאום של כלל פעילות הסיכול והאיסוף הביטחוניים לצורכי הגנה בסייבר.

3. **מרכז לאומי לניהול המערכה, לזיהוי ולחקירה (מרכז אופרטיבי מדינתי).** המרכיב השלישי הוא הניהול הכולל של מערכת ההגנה במרחב הקיברנטי. האתגר המרכזי של המרכז הלאומי שיופקד על כך הוא ליצור תמונת מצב הגנתית משותפת ומתוכללת (אינטגרטיבית) של כל האיומים הקיברנטיים על ישראל. לשם כך עליו להיות ציר מקשר בין שכבות ההגנה. נוסף על כך, במקרה של תקיפה משמעותית נגד אחד או יותר ממרחבי ההגנה יהיה על המרכז הזה לגבש תמונת מצב, לנהל את האירוע באופן מרוכז, להגדיר סדרי עדיפויות וריכוזי מאמץ ובמקביל להפעיל צוותי זיהוי וחקירה. למרכז הלאומי יש חשיבות אסטרטגית בהיותו מרכז העצבים בעיתות שגרה, בעת אירוע ביטחוני ובמצבי חירום. המרכז הזה הוא הגרעין שינחה את גופי הביצוע במשימת ההגנה כפי שהוגדרו על ידי המטה הקיברנטי הלאומי. כדי להקים ולתפעל מרכז כזה ביעילות ובמהירות מוצע להטיל על צה"ל לפקד עליו על בסיס פיקוד סייבר ייעודי.

המטה הקיברנטי הלאומי

במרחב הקיברנטי מתנהלת כיום מלחמה גם בין מדינות שכלל אינן מצויות במצב מלחמה זו עם זו. המציאות המטרידה הזאת מחייבת את ישראל לפעול במהירות. הרמות הבכירות ביותר מכירות בחשיבותו של המרחב הקיברנטי, וכבר הוזכרו כאן דבריו של ראש הממשלה בנימין נתניהו שאיום הסייבר הוא אחד מחמשת האיומים המרכזיים על הביטחון הלאומי של ישראל. אף ניכר מאמץ לתת מענה לאיום הזה, והוזכרה כאן הקמתם של המטה הקיברנטי הלאומי ושל היחידות הייעודיות במערכות הביטחון שאמורות לספק הגנה מפני מתקפות סייבר. מה שיש כעת לעשות הוא לגבש מתווה ארגוני ולממשו. בשלב הזה מוצע להטיל על צה"ל להיות מוביל המערך כולו באמצעות פיקוד הסייבר.

ניתן לשער כי כאשר תתרחש תקיפת סייבר משמעותית על התשתיות הלאומיות, ייקרא צה"ל לסייע, כפי שהוא נקרא לסייע בשריפה בכרמל בדצמבר 2010 ובסופת השלגים של דצמבר 2013 וכפי שהוא צפוי להיקרא במקרה של רעידת אדמה חזקה.

הגישה הזאת שלפיה המדינה מטילה את האחריות להגנת המרחב הקיברנטי על הצבא אומצה בכמה ממדינות המערב. כך, למשל, בארה"ב. נאט"ו הקימה מרכז סייבר אזורי שמשותף לכל המדינות החברות בארגון. אסטוניה, שחוותה על בשרה מתקפת סייבר משמעותית, הפכה כתוצאה מכך לאחת המדינות המתקדמות בעולם בתחום של הגנת סייבר. את ההגנה על המרחב הזה היא הטילה על הצבא.

חשוב להטמיע בכל הרמות את ההבנה שהשימוש בסייבר לצורכי לחימה ותקיפה אינו תיאורטי. כפי שחיל האוויר מגן על המרחב האווירי של המדינה, חיל הים מגן על המרחב הימי, והפיקודים המרחביים מגינים על הגבולות היבשתיים, כך יש להתארגן להגנה במרחב הסייבר. מאחר שמאחורי כל התקפות הסייבר המדינתיות עומדים הצבאות של אותן המדינות, על ישראל להעמיד מול ההתארגנות הצבאית ההתקפית הזאת התארגנות צבאית הגנתית. יתר על כן, ההתפתחויות בתחום הזה הן מהירות מאוד. כדי למנוע מצב שבו נהיה מופתעים עלינו להיערך במהירות רבה מתוך

הבנה שמדובר במצב חירום. אין ספק שהגוף המוכשר ביותר להקמת מענה מהיר בישראל הוא צה"ל - בין היתר בשל גמישותו הארגונית וגישתו הישירה למאגרי כוח האדם האיכותיים ביותר.

הניסיון לקבוע כבר עכשיו מתאר ארגוני אזרחי סופי עלול להוביל למאבקי כוח בין הגופים השונים - מאבקים שעלולים לחבל בשיתוף הפעולה ביניהם ובאפקטיביות של המענה. הניסיון מלמד שצה"ל הוא במקרים רבים גורם מאחד ומלכד. אם תוטל עליו המשימה, יגדלו מאוד הסיכויים לרתום את כל הגופים לעבוד במהירות הנדרשת ובשיתוף פעולה ביניהם. נוסף על כך, צה"ל בהיותו גוף ביצועי ומשימתי יצליח לעמוד במשימה בזמן.

במשק פועלות חברות רבות שחיוניות לתפקוד המגזר הביטחוני בכלל והצבאי בפרט. לכן מקפיד צה"ל לערוך תרגילים בתחום לוחמת הסייבר שאליהם הוא רותם את כל החברות הרלוונטיות בתחום. עצם העובדה שצה"ל מוביל את המאמץ הזה מקרין על חשיבות הנושא, רותם את ההנהלות הבכירות ומעודד שיתופי פעולה בין חברות עסקיות.

סיכום והמלצות

נוכח איומי הסייבר על ישראל יש לאמץ דפוסי חשיבה חדשים, ליזום התארגנויות חדשות ולהקפיד על שיתופי פעולה בין־ארגוניים.

המלצות

1. יש להקים רשות אזרחית להגנה בסייבר שתקבל אחריות להגנה על כל הגורמים במגזר האזרחי שפועלים בסייבר. הרשות האזרחית הזאת תהיה כפופה למטה הקיברנטי הלאומי.
2. יש לחזק את יחידת הסייבר במשטרה כדי למנוע ולחקור פשיעה במרחב הקיברנטי.
3. יש להקים מחלקה ייעודית שעליה יוטל לכוון ולתאם את המודיעין בסייבר. המחלקה הזאת תהיה כפופה למטה הקיברנטי הלאומי.
4. יש להקים בצה"ל פיקוד סייבר אופרטיבי שיהיה אחראי לשני תחומים:
   א. פעילות בכל ממדי הסייבר הצבאי בהתאם לדוקטרינת קולמן: הגנה, איסוף, סיכול, התקפה.[30]
   ב. ניהול של אירוע חירום לאומי בתחום הסייבר - במיוחד בתחומי הזיהוי והחקירה. ראש המטה הקיברנטי הלאומי הוא שיכריז על מצב חירום לאומי.
5. יש לגבש אסטרטגיה מדינית להגנה, לפעילות ולרציפות תפקודית במרחב הקיברנטי.
6. יש לשלב את המרחב הקיברנטי בתפיסת הביטחון של ישראל.
7. יש לגבש את איום הייחוס למתקפת סייבר נרחבת ולתרגל מתן מענה שלם להתמודדות עם איום כזה. במילים אחרות: יש להגדיר מיהם אויביה של ישראל בתחום הסייבר ולהיערך לבלימת ניסיונותיהם לערוך מתקפות סייבר על ישראל.

כאמור, קיים הכרח להקים פיקוד סייבר בצה"ל. הפיקוד הזה נדרש לפעולה מתואמת ומשולבת בכל הממדים שצוינו בדוקטרינת קולמן: הגנה, איסוף, סיכול והתקפה ולהביא אותם לכלל שלמות מבצעית אחת. ראוי שפיקוד הסייבר יהיה מצוי בתוך הליבה המבצעית של צה"ל וייחשב לאופרטור - מפעיל כוח - לכל דבר ועניין ממש כמו מפקד פיקוד ביבשה או מפקד חיל האוויר או מפקד חיל הים.

אלה הם החלופות שיעמדו בפני מקבלי ההחלטות בעניין הזה:

1. הקמת פיקוד חדש.
2. הקמת הפיקוד על בסיס אגף המודיעין.
3. הקמת הפיקוד על בסיס אגף התקשוב.

מבחנו האמיתי של פיקוד הסייבר יהיה ניהול אירוע של מתקפת סייבר נרחבת נגד ישראל. לקראת אירוע בסדר גודל כזה יידרש פיקוד הסייבר להתארגנות, למקצועיות, לגיבוש תפיסה ותורה בתיאום עם הארגון הלאומי להגנת המגזר האזרחי בסייבר ולתרגול כלל המערכים המדינתיים תחת קורת גג אחת בניצוחו של המרכז הלאומי לניהול המערכה ובפיקודו של מפקד פיקוד הסייבר.

מן הראוי שהתובנות האלה יאומצו על ידי גופי בניין הכוח הביטחוניים והצבאיים במדינה וייעשה בהן שימוש בתהליכי ההתכוננות לאתגרים העומדים לפתחנו. אסור שנופתע בזירה הזאת, כפי שכבר קרה לכמה מדינות שלא היו ערוכות כנדרש.

הערות

1. המרחב הקיברנטי הוא המתחם הפיזי והלא פיזי שנוצר או שמורכב מהגורמים הבאים: מערכות ממוכנות ורשתות, תוכנות, מידע ממוחשב, תוכן, נתוני תעבורה ובקרה והמשתמשים בכל אלה.
2. המרחב הקיברנטי כבר מוגדר בצבא ארה"ב מרחב הלחימה החמישי.
3. ככל שהמדינות המודרניות מגבירות את הישענותן על מערכות מחשוב מתקדמות, כך הן חשופות יותר לתקיפה ולשיבוש במרחב הקיברנטי.
4. יוסי גורביץ, "ממשלת ארה"ב מפחדת מההאקרים המטורפים של איראן", **כלכליסט**, 4 במרס 2013, http://bit.ly/Z18Jlk
5. רפאל קאהאן, "לראשונה אובמה מאשים את סין בהתקפות הסייבר על ארה"ב", **כלכליסט**, 14 במרס 2013, http://bit.ly/Z76ThU
6. קישוריות מערכות המידע ומערכות השליטה והבקרה ברמה המערכתית וברמה הטקטית.
7. מחלקת הגנות בסייבר הוקמה באגף התקשוב במסגרת הקמתו של מטה הסייבר של צה"ל.
8. בעבר התבססה תפיסת הביטחון של ישראל על שלוש רגליים: הרתעה, התרעה, הכרעה. כעת ישנה המלצה להחליף את המושג "הכרעה" במושג "התקפה" כדי להדגיש את תפיסת הניצחון.
9. שמואל אבן ודוד סימן טוב, **לוחמה במרחב הקיברנטי - מושגים, מגמות ומשמעויות לישראל**, מזכר 109, המכון למחקרי ביטחון לאומי, 2011, http://bit.ly/HUY5bJ
10. **שם**
11. **שם**
12. יורם שווייצר, גבי סיבוני ועינב יוגב, "המרחב הקיברנטי וארגוני הטרור", **צבא ואסטרטגיה**, כרך 3, גיליון 3, דצמבר 2011, http://bit.ly/1d1XQsU
13. **אבן וסימן טוב**, עמ' 44
14. על המלחמה ראו: יעקב קדמי, "מלחמת חמשת הימים", **מערכות** 449, יולי 2013, עמ' 48-52, http://maarachot.idf.il/PDF/FILES/2/113232.pdf
15. **NATO** "New Threats - The Cyber Dimension", **Review**, 11.9.2011, http://bit.ly/1dfrC9e
16. **אבן וסימן טוב**, עמ' 38
17. בתחילה סברו חוקרי האבטחה שמדובר בתולעת שנועדה לריגול תעשייתי, אולם חוקר אבטחה בשם ראלף לנגנר כתב לאחר ניתוח הקוד של סטוקסנט שמדובר בתולעת למטרות חבלה.
18. "סימנטק: וירוס סטוקסנט ששימש לתקיפת איראן פעיל כבר מ־2007", **דה מארקר**, 27.2.2013
19. "איראן מאשימה: ישראל וארה"ב יצרו את תולעת המחשבים סטוקסנט", **הארץ**, 16.4.2011, www.haaretz.co.il/news/world/1.1171376
20. **אבן וסימן טוב**, עמ' 37
21. גבי סיבוני, "מה עומד מאחורי לוחמת הסייבר של סין", **צבא ואסטרטגיה**, כרך 4, גיליון 2, ספטמבר 2012, http://bit.ly/1hNdSco
22. ניצן סדן, "ארה"ב: צבא ההאקרים הסיני פרץ לרבע מהחברות האמריקאיות שפועלות במדינה", **כלכליסט**, 29.3.2013, http://bit.ly/ZIUCAW
23. יצחק בן חורין, "יחידה סודית בצבא סין פרצה למחשבים בארה"ב", **ynet**, 19.2.2013, http://bit.ly/XK1Ro1
24. "שלוש רשתות טלוויזיה ושני בנקים בדרום־קוריאה נפגעו במתקפת סייבר", **הארץ**, 20.3.2013, http://bit.ly/YXGDGY
25. רועי גולדשמידט, **המרחב הקיברנטי וההגנה על תשתיות חיוניות**, מרכז המחקר והמידע של הכנסת, ירושלים, 2013
26. רוברט מילר ודניאל קיהל, "המרחב הקיברנטי ו'הקרב הפתוח' במלחמה של המאה ה־21", **תצפית**, 61, 2011
27. הנתונים התקבלו ממטה התקשוב הממשלתי ומהנהלת ממשל זמין.
28. החלטת הממשלה ב/84 מיום 11.12.2002, http://bit.ly/1eb38zs
29. גילי כהן, "הסייבר - זירת הלחימה החדשה של צה"ל", **הארץ**, 4.3.2013, www.haaretz.co.il/news/politics/1.1946156
30. על דוקטרינת קולמן ראו: http://bit.ly/1d9N1Ti