לכבוד **11 ביולי 2018**

משרד ראש הממשלה

מערך הסייבר – היועץ המשפטי

באמצעות אתר קשרי ממשל

הנדון: <u>הערות לתזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי התשע"ח-2018</u>

<u>הערות מרכז המחקר להגנת הסייבר של האוניברסיטה העברית</u>

בתגובה לתזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי התשע"ח-2018 (להלן: "**התזכיר**"), נבקש להביא את הערותיהם של קבוצת חוקרים ממרכז המחקר להגנת הסייבר, הכוללת את עו"ד דבורה האוסן-כוריאל, עו"ד דן עפרוני, ד"ר עמית שניאק ועו"ד עמיר כהנא.

מפאת סד הזמנים הקצר שנקבע להערות הציבור, ומטעמי יעילות התייחסותנו לא תוכל להקיף את כלל הסוגיות העקרוניות שהתזכיר מעלה המחייבות בירור והעמקה. כך למשל, לא התייחסנו לכלל הסעיפים המקנים למערך הסייבר סמכויות שונות לפגוע בזכויות אדם, בין אם לפרקי זמן קצרים, ללא אישור שיפוטי ובין אם לפרקים ארוכים יותר ובפיקוח שיפוטי. אנו מניחים שהסדרים אלו, יזכו להתייחסותם **הביקורתית** והמקיפה של גופים אחרים שזהו מוקד עיסוקם. המרכז מקיים קבוצת מחקר הבוחנת חלק מהסדרי הרגולציה המוצעים בחוק וממצאי המחקר יתפרסמו בעתיד.

על כן, ראינו לצמצם את התייחסותנו לנושאים עקרוניים אחרים מאלו ונעשה זאת בקצירת האומר – נשמח להרחיב בע"פ ובכתב ככל שיהיה עניין בכך.

א. <u>ייעודו של מערך הסייבר – מתן הגנה לאזרחי ותושבי ישראל במרחב הסייבר</u>

סעיף 2 לתזכיר[1] מגדיר את מערך הסייבר כגוף בטחוני מבצעי, שייעודו הגנת מרחב הסייבר וקידום ישראל כמובילה עולמית בתחום הסייבר. האיפיון המוצע אינו ברור: האם מדובר בהוספת עוד גוף בטחוני לשורה של אלה הקיימים (צה"ל, מוסד, שב"כ) או שמא מדובר בגוף אזרחי שעובד בשותפות עם גורמים הביטחוניים הקיימים? אופי הארגון ותכליתו אינם ברורים בניסוח זה. אנו מציעים לקבוע את הגנת מרחב הסייבר כייעוד יחידי, החלק המתייחס להובלה ב-"תחרות" עולמית אינו ממין העניין, ולא ראוי לטעמנו שיכלל בדבר חקיקה. אפיון כזה מתאים יותר להיכלל במסגרת חזון ארגוני, בו ניתן ואף רצוי להציב יעדים הנוגעים לחדשנות ויצירתיות בארגון, ולמובילות השוואתית.

אין באמור לעיל כדי לשלול מהמערך סמכות לעסוק במחקר ופיתוח, ככל שאלה ממוקדים בענייני ההגנה בסייבר. צה"ל ושאר גופי הביטחון בישראל יודעים לעשות כן ובהצלחה ראויה לציון במאמץ פנים ארגוני ו/או בשיתופי פעולה עם גופי מחקר ותעשייה אזרחיים, ואין סיבה נראית לעין להוציא את מערך הסייבר מן הכלל.

אם יוחלט להותיר את ייעוד המובילות העולמית על כנו, כי אז נעיר שנראה כי התזכיר אינו מקנה לארגון סמכויות הנובעות באופן ישיר מחלקו השני של ייעודו, "קידום ישראל כמובילה עולמית בתחום הסייבר" – כמו למשל, סמכויות הנוגעות להכשרת כוח אדם או לקידום מחקר ופיתוח. עם זאת, מערך הסייבר (בגלגוליו הקודמים כמטה הסייבר במשרד ראש הממשלה) פעל בעבר בהקשרים אלו,[2] רצוי לפרט אילו

---

[1] כל ההפניות לסעיפים ופרקים בגוף ההערות מתייחסות לסעיפי ולפרקי התזכיר.

[2] ר' לדוגמא החלטת ממשלה 528 (הטבה למעסיקים בתחום הגנת הסייבר בקריית הסייבר הלאומית) (6.9.2015) http://www.pmo.gov.il/SiteCollectionDocuments/cyber/DES528.pdf; פעולות לקידום כוח אדם מקצועי בתחום הסייבר, כמתואר אצל הרשות הלאומית להגנת הסייבר, "סיכום שנות ההקמה 2016-2017" בעמ' 29 https://www.gov.il/BlobFolder/news/summary/he/סיכום%20שנתיים%20הרשות%20הלאומית%20להגנת%20הסייבר.pdf

סמכויות וכלים ספציפיים מוקנים למערך על-מנת לממש תכלית זו, וכיצד אלו מתממשקים עם סמכויותיהן של רשויות אחרות במדינה, למשל בתחומי המיסוי, פיתוח התשתיות, ניהול הסחר הבינלאומי וקשרי החוץ של ישראל.

החוק המוצע הוא למעשה חוק המבקש להקים גוף בטחוני חדש בישראל, נוסף על הקיימים ולייעד לו את האחריות על ההגנה בסייבר. אם כך הם פני הדברים יש להגדיר בחוק או מכוח חוק את גבולות הגזרה של האחריות הארגונית, בייחוד בין המערך לבין צה"ל ושב"כ. זאת בשים לב לכך שפעילות עוינת במרחב הסייבר לפעמים תוגדר צבאית, לפעמים מסחרית, לפעמים אזרחית. יש להכיר בטשטוש גבולות מסורתיים אלה, ונדרשת כאן חשיבה ואף תעוזה כדי להגיע לרמת ההבהרה הרגולטורית הנדרשת בדגש להבהרות באשר לסמכויות בעת שגרה, חירום ומלחמה.

מהגדרת "הגנה בסייבר" - "מכלול הפעולות הנדרשות למניעה, להתמודדות ולטיפול בתקיפת סייבר או איום סייבר..." ומתפקידי המערך – "לנהל, להפעיל ולבצע בהתאם לצורך את מאמצי ההגנה לאומיים האופרטיביים כנגד תקיפות סייבר" משתמע שגם פעולות סיכול ומניעה תהנה באחריות המערך. במילים אחרות, משתמע כי המערך יהיה מוסמך להפעיל כלים של הגנה אקטיבית, לרבות כלים בעלי אופי התקפי. האם זו אכן כוונת המחוקק? האם למערך תהיינה יכולות תקיפה בסייבר? האם יש, אם כן, כוונה לגרוע מצה"ל, האמון על הגנת המדינה, את חזית הסייבר, ומהשב"כ את הסיכול בסייבר? רצוי להתייחס להבדלים במענה ובהתמודדות בין תקיפות שמקורן בגורמי פשיעה לבין תקיפות מדינתיות ושל גורמי טרור, שגופי המודיעין והצבא אמונים על התמודדות איתם.

יתר על כן, ספק אם תרחיש של תקיפת סייבר יהיה מוגבל אך ורק למרחב הסייבר. נהפוך הוא, משחקי לחימה שנערכים בפורומים שונים בעולם כוללים תרחישים של מערכה משולבת , ביבשה, באוויר, בים ובסייבר. כיצד ישתלב המערך במערכה כזו? מי הגורם שיפקד על חזית הסייבר, בחירום כמו גם בשגרה? התשובות חייבות להיגזר מתיחום מוגדר ומדויק של אחריות בין הגופים השונים.

ב. <u>התפיסה של המערך כ"מאסדר – על"</u>

לצד מאפייניו הביטחוניים-מבצעיים המוצעים של הארגון, התזכיר מציע לקבוע למערך הסייבר גם תפקיד כמאסדר-על (או מאסדר ישיר, בהתאם לעניין) במגזרים שונים במשק. אופיו ההיברידי של הארגון, אם יוחלט לשמרו, מחייב תיחום מפורט הרבה יותר של הסמכויות המוקנות לעובדיו בהתאם לתפקידם, ולהבחנה ברורה יותר בין הזרוע הביטחונית לבין הזרוע הרגולטורית של המערך.[3] בנוסף, יש להיזהר מההשפעה של החשאיות האופפת את הארגון על הפעילות הכלכלית אותה הוא מאסדר ו/או מקדם.

בהיבטי השת"פ הבינלאומי, מן הראוי שהתקשרויות פורמליות מהסוג המוצע בתזכיר תהיינה בתיאום מלא עם הגורמים הרלוונטיים במשרד החוץ. בנוסחו הנוכחי, ההסדר המוצע מנתק את מערך הסייבר משיקולי קשרי חוץ של מדינת ישראל, כפי שהם מתגבשים בקרב משרד החוץ, המשרד הממונה על קשרי החוץ של המדינה באופן קבוע .

ג. <u>מענה למאפיינים הייחודיים של איום הסייבר</u>

הצורך בתיאום בין הגופים הביטחוניים המיוחדים עולה בהתייחס למאפיינים הייחודים של איום הסייבר. הקושי בייחוס איומי סייבר לתוקפים ולמטרות מסוימות, מחייב הגדרה של ממשקים וסמכויות בין הצבא, המשטרה, שירות הביטחון הכללי, המלמ"ב ומערך הסייבר – לעניין שיתוף במידע והיקפו, ולתיאום פעולות בין הארגונים השונים. סעיף 37 של התזכיר, לפיו כאשר ראש המערך נוכח לדעת שמניעת הפגיעה באינטרס חיוני או צמצומה מחייב פעולה של בעל סמכות נוסף, עליו להודיע על כך לאותו בעל סמכות, וזה יקבע איש קשר לסיוע למניעת הפגיעה, מותיר את עיצוב הממשק בין המערך לבעל-הסמכות הרלוונטי למועד האירוע, דבר אשר עלול לפגוע באפקטיביות המבצעית בזמן אמת. נוסף להוראה זו, יש להגדיר במפורש את הממשקים וחלוקת הסמכויות בין המערך לבין הגופים המיוחדים האחרים, על מנת למנוע עיכובים הנובעים ממחלוקות בין-ארגוניות.

אופיים של איומי הסייבר עשוי לייצר מצב שבו החריג שבסעיף 36 יהפוך להיות הכלל. בהינתן קבועי הזמן הקצרים בקשר עם תקיפות סייבר והטיפול בהן, סביר להניח כי הצורך בהפעלת הסמכויות שבפרק ג' סימן ב' עלול להתעורר בנסיבות דחופות (לפי התזכיר, אף ללא שהות מספקת על-מנת לפנות לבית-המשפט

[3] נעיר כי התזכיר מניח תשתית לכך, בהקנותו לראש-הממשלה סמכויות ביחס למערך הסייבר, שמקבילותיהן מסורות בחוק השב"כ לראש השב"כ, אך אין במסגרת הגמישה של לשון התזכיר כדי להבטיח שראש-הממשלה יפעיל סמכויות אלו לתכלית זו.

בבקשה לצו). משכך, יש לתת את הדעת על חיזוק מנגנוני הבקרה הפנימיים והחיצוניים שבסעיף, באופן שיצמצם את ניצולו לרעה. ושיאפשר פיקוח אמיתי ואפקטיבי על פעילות המערך בהקשר זה.

ד. <u>ריכוז סמכויות בידי ראש הממשלה</u>

מאפייניו הביטחוניים של מערך הסייבר באים, לידי ביטוי, בין השאר, בסעיפים בתזכיר הלקוחים מנוסח חוק שירות הביטחון הכללי, התשע"ב-2002 (להלן: "**חוק השב"כ**"). עובדי המערך או הפועלים מטעמו בתפקידים מסוימים, פטורים, בדומה לעובדי השב"כ, מאחריות פלילית או אזרחית למעשה או מחדל שנעשה בתום לב ובאורח במסגרת תפקידם ולשם מילויו,[4] וכן חלות עליהם הגבלות דומות לאלו החלות על עובדי השב"כ.[5] ראש המערך ממונה באופן דומה לראש השב"כ.[6]

ואולם, בהשוואה לחוק השב"כ, נראה כי התזכיר מקנה לראש הממשלה **סמכויות רחבות מדי** ביחס למערך הסייבר. אין הוראות מקבילות בחוק השב"כ ביחס לסמכות ראש הממשלה לקבוע בכללים משרות או תפקידים בהם נדרשת מומחיות מיוחדת המאפשרת את העסקת גם מי שאינו עובד מדינה;[7] ראש הממשלה רשאי לקבוע בתקנות הוראות בדבר משטר ומשמעת שיחולו במערך.[8] יתר על כן, גם בנושאים מהותיים הנוגעים לתכליות וייעודי המערך, מוקנות לראש הממשלה סמכויות מיוחדות – ראש הממשלה ראשי לקבוע בצו אינטרס חיוני נוסף על אלו המנויים בחוק,[9] וכן להוסיף על תפקידי המערך שבחוק.[10] בחוק השב"כ, הסמכות לשנות את תפקידי השב"כ ניתנה לממשלה, ובאישור ועדת הכנסת לענייני השירות.[11] חלק ניכר מסמכויות ראש הממשלה שבתזכיר אינו מותנה בהסכמתו או בשיתופו של גורם נוסף,[12] ולכל היותר מותנות סמכויות אלו בהתייעצות בלבד עם השר הממונה, ולא בהסכמתו.[13] יש מקום לצמצם סמכויות אלו, בחלק מהן לא להסתפק בהתייעצות אלא לדרוש את הסכמת שר המשפטים, ובחלקן להעבירן לאישור לפיקוח ועדת המשנה של ועדת חוץ וביטחון או, למצער, הקבינט הביטחוני. בכל מקרה, הצורך במנגנוני פיקוח מוסדרים מראש על פעילות כאמור של הרחבת סמכויות חריגות – ואולי גם הגבלתן בזמן – ראוי ונדרש.

ה. <u>פיקוח ובקרה על הפעלת הסמכויות בתזכיר</u>

לנוכח המתואר לעיל, מן הראוי לבחון את מנגנוני הפיקוח והבקרה על מערך הסייבר שמציע התזכיר, וזאת מטעמי שלטון החוק במדינה דמוקרטית.

ראשית, בשים לב למאפייניו הביטחוניים של מערך הסייבר, נראה כי היקף הביקורת והפיקוח המוצעים בתזכיר הינם חסרים בהשוואה לאלו המצויים בחוק השב"כ. להבדיל מהשירות, מערך הסייבר אינו נתון לפיקוח פרלמנטרי[14] ודיווחיו השנתיים של ראש המערך מיועדים לעיניו של ראש הממשלה בלבד[15] (אשר יש לצפות כי יהיה מעורה די הצורך בענייני מערך הסייבר ממילא, בהתחשב בהיקף הסמכויות המוקנות לו בתזכיר).

הגם שחוק הביקורת הפנימית חל על מערך הסייבר, לא ראינו התייחסות לו בתזכיר. יש למנות **מבקר פנים** למערך בדומה להסדר שבחוק השב"כ,[16] המוסיף על הוראות חוק הביקורת הפנימית[17] ומגדיר את אורך הקדנציה של המבקר (שבסופה לא ימלא תפקיד אחר בשירות), מחדד את אופן מינויו, מתנה את השעייתו באישור ועדת השרים, ומרחיב את מעגל הגורמים להם הוא מגיש את דיווחיו השנתיים.[18]

---

[4] ס' 8 לתזכיר, השוו עם ס' 18 לחוק השב"כ.

[5] ס' 7 לתזכיר, השוו עם ס' 20 לחוק השב"כ. ואולם, ההגבלות שרשאי ראש-הממשלה לקבוע מכוח ס' 20 לחוק השב"כ הינן "ככל שהדבר דרוש לשם מילוי תפקידי השירות, להבטחת טוהר המידות בשירות, או לשם שמירת בטחונם האישי של עובדי השירות ועובדיו לשעבר", בעוד שנוסח הסעיף המקביל בתזכיר הינו "לשם מילוי תפקידי המערך, להבטחת טוהר המידות במערך, ולהבטחת אמון הציבור במערך". אנו חוששים שמא תכלית "הבטחת אמון הציבור במערך" שבתזכיר עשויה לשמש אצטלא להגבלות אשר יימנעו חשיפת מקרי שחיתות או ניצול לרעה של סמכויות המערך. יתר על כן, מן הראוי להקפיד על אחידות בנוסח החוקים ולסטות ממנה רק להגשמת התכליות המיוחדות של כל ארגון.

[6] השוו ס' 4(א) לתזכיר עם ס' 3(א) לחוק השב"כ.

[7] ס' 5(ב) לתזכיר.

[8] ס' 5(ג) לתזכיר, השוו עם ס' 14 לחוק השב"כ המקנה סמכות זו לראש השירות.

[9] ס' 1 לתזכיר, ס"ק 8 להגדרת 'אינטרס חיוני'.

[10] ס'3(6) לתזכיר.

[11] ס' 7(ב)(6) לחוק השב"כ.

[12] למעט ס' 16(ב), 38(ב), 25(ח), 18(6), 17(ה), 4(א).

[13] לדוגמא ס'18(5), 47(א)-(ב), 57(ג), 63.

[14] ר' ס'6 לחוק השב"כ.

[15] ס' 4(ה) לתזכיר, והשוו עם ס' 12 לחוק השב"כ.

[16] ס' 13 לחוק השב"כ.

[17] חוק הביקורת הפנימית, התשנ"ב-1992, ס"ח 1395 (9.4.1992).

[18] ס' 13 לחוק השב"כ. ר' הטקסט המפנה להי"ש 72-67 אצל אריה רוטר "על יעודם ותפיסת תפקידם של שומרי הסף בארגוני המודיעין, המקרה של שירות הביטחון הכללי" **עיונים בביטחון לאומי 6**, (2008).

מפקח הפרטיות הפנימי הינו יוזמה ברוכה, אך יש לחזק מוסד זה. כך למשל, לקבוע כי מינוי והפסקת כהונת המפקח מותנים בהתייעצות עם רשם מאגרי המידע, ויש אף לשקול להתנותם **בהסכמתו**. בדומה להוראות החלות על הועדה המפקחת, על התזכיר להדגיש כי המפקח במילוי תפקידו אינו נתון אלא למרותו של הדין.[19] כן רצוי שלא להתיר למפקח למלא כל תפקיד אחר,[20] ולהרחיב את מעגל הגופים להם הוא מדווח,[21] לרבות לוועדה פרלמנטרית מתאימה.

נראה כי אין די במנגנוני הפיקוח והבקרה המוצעים בתזכיר. חרף הסמכויות המוקנות **לוועדה המפקחת,**[22] התזכיר אינו מקצה לה משאבים על-מנת לממשן (כזכור, התזכיר מציין כי אין לחקיקתו השלכות תקציביות ישירות).[23] סמכויות הועדה מוגבלות לפיקוח על השפעת פעילות המערך על הזכות לפרטיות, בעוד שיש מקום להרחיב את היקף הפיקוח לכל היבטי פעילות המערך, אשר עלולה לפגוע בזכויות נוספות. נראה כי מינוי נציג ראש מערך הסייבר כמזכיר לוועדה[24] יש בו כדי לפגוע באי תלותה. יש לשער כי נציג הציבור המומחה לתחומי הגנת סייבר וביטחון לאומי, עשוי להיות בעל זיקה בעייתית למערך. מנגד, הוועדה כוללת שני חברים הממונים שלא בהתבסס על מומחיות ספציפית (משפטן בכיר ונציג היועץ המשפטי לממשלה) – ויש לבחון אם העדר הרקע המקצועי עשוי להעיב על תפקוד הוועדה. הוועדה מדווחת לראש הממשלה בלבד,[25] ויש להרחיב את מעגל הגופים להם היא מדווחת, לרבות לוועדה פרלמנטרית מתאימה והציבור בכלל. ישראל לא תהיה חלוצה בהקשר זה, יש מספר מדינות, ובכללן בריטניה והולנד, שמשתפות את הציבור באופן קבוע בנעשה על ידי הממשלה בהיבטים נבחרים של תחום הסייבר.[26]

הפעלת חלק מהסמכויות שבפרק ג׳ כפופה לביקורת שיפוטית. יש לשקול הכשרת שופטים לדון בענייני סייבר, בהתחשב במומחיות הנדרשת לתחום זה, ולוודא כי הכשרה זו מועברת באמצעות גורם אובייקטיבי, על מנת לשמור על עצמאות השופטים. כמו כן, בשים לב לכך שהצווים הניתנים הם בקשר עם ביצוע פעולות בחומר מחשב, העשוי להשפיע הן על אינטרסים הקשורים בזכות לבפרטיות והן על אינטרסים אחרים – יש מקום לשקול להקנות את סמכות הדיון בצווים אלו לבית-משפט מחוזי.[27]

בשים לב למאפייניו ההיברידיים של מערך הסייבר, יש לוודא כי עקרון צמידות המטרה נשמר גם ביחס למידע שנאסף מחוץ למערך הגילוי (בהתאם להוראות ס׳17(א)). נראה כי ס׳ 40 לחוק מאפשר חריגה מעקרון זה באופן הפותח פתח לזליגת מידע (intelligence creep) בין הגופים המיוחדים, ולעתים ללא הצדקה ברורה.[28]

ו. <u>סיכום</u>

לסיכום, אנו סבורים שדבר חקיקה המבקש להקים גוף בטחוני-מבצעי חדש, בעל טווח כה רחב של פעילות וסמכויות מוצעות, רצוי שיקפיד על תיאום ואחידות עם חקיקה קיימת. יש לתת את הדעת על גבולות הגזרה וחלוקת האחריות בין המערך לבין הגופים המיוחדים האחרים, ולחזק משמעותית את מנגנוני הבקרה והפיקוח המוצעים בתזכיר, למצער באופן שיקבילם למנגנוני פיקוח ובקרה סטטוטוריים קיימים, אם לא מעבר לכך – בשים לב לתפקיד המוצע של הארגון כרגולטור-על חדש במדינה.

כאמור, נשמח לפרט ולהרחיב לגבי כל אחת מהנקודות שהועלו במסמך זה.

---

[19] ס׳ 13(ו) לתזכיר.

[20] להבדיל מההוראה בס׳ 10(ה) לתזכיר, לפיה המפקח רשאי לעסוק בעיסוק אחר כל עוד עיסוק זה אינו עלול להעמיד אותו בחשש לניגוד עניינים.

[21] לפי ס״ק 11(4), 11(7) לתזכיר.

[22] ס׳ 15-13 לתזכיר.

[23] מבקרים מצביעים על הקצאה חסרה של משאבים למנגנוני בקרה שונים על ארגונים ביטחוניים כהסבר לחוסר האפקטיביות שלהם. ביחס לארגוני מודיעין ר׳ לדוגמא Kent Roach, *"Review and Oversight of Intelligence in Canada"* 183 in ZACHARY K. GOLDMAN AND SAMEUL J. RASCOFF, EDS., GLOBAL INTELLIGENCE OVERSIGHT (2016); Russell A. Miller, *"Intelligence Oversight – Made in Germany"* 270 GOLDMAN AND RASCOFF, Ibid.

[24] ס׳ 13(ב) לתזכיר.

[25] ס׳ 14(א) לתזכיר.

[26] ר׳ Netherlands Cyber Security Assessment, 2017 ו-UK National Cyber Security Centre Annual Review 2017.

[27] השוו עם חוק סמכויות לשם מניעת ביצוע עבירות באמצעות אתר אינטרנט, תשע״ז-2017. לחלופין, השוו עם ס׳ 6 לחוק האזנת סתר, תשל״ט-1979, לפיו האזנת סתר למטרות מניעת פשיעה כפופה לצו מאת נשיא או סגן נשיא בית משפט מחוזי. הגם שצו לפי חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס״ח-2007 ניתן על-ידי בית-משפט השלום, נראה כי הערכאה המתאימה לדון בצווים לביצוע פעולות בחומר מחשב היא בית-המשפט המחוזי – הן בהתייחס למידת הפגיעה בפרטיות הקשורה בסוג הנתונים (הפעולות המבוקשות אינן מוגבלות לנתוני תקשורת או ל-metadata בלבד, והן בהתייחס לטיבן - להבדיל מהאזנת סתר או מקבלת נתוני תקשורת מבעלי רישיון בזק, שהינן פעולות בעלות אופי פאסיבי שאין בו כדי להשפיע על המידע המיורט, פעולות בחומר מחשב עשויות לכלול גם שינוי נתונים ומתן הוראות למחשב).

[28] ר׳ לדוגמא ס׳ 40(א) סייפא – מדוע ׳הפרעה לעובד ציבור׳ מצדיקה גילוי ידיעות או מסמכים שנמסרו לעובדי המערך מכוח תפקידם׃