הכנסת
ועדת החוץ והביטחון

דין וחשבון בנושא

בחינת חלוקת האחריות והסמכות בנושא הגנת הסייבר בישראל

דו"ח לא מסווג

תמוז התשע"ו - אוגוסט 2016

מסר מרכזי

1. ועדת המשנה של ועדת החוץ והביטחון לנושא ההגנה בסייבר ניהלה בשנה האחרונה שורה של סיורים ודיונים כדי ללמוד ולפקח על אופן ההיערכות המדינתית להגנת הסייבר, ולבחון את משמעויות החלטת הממשלה על הקמת רשות הסייבר הלאומית ואופן מימושה.

2. הוועדה נחשפה להשקפות עולם שונות ביחס לאסטרטגיית ההגנה למול איום הסייבר, כמו גם למחלוקות, מאבקי כוח, ובמקרים מסוימים אף היעדר שיתוף פעולה הדדי בין הרשות וגופי הביטחון, כאשר נראה כי **לאחרונה עלו הצדדים על פסים של הידברות מועילה**.

3. מטרת הדו"ח, לבחון את חלוקת האחריות והסמכויות הרצויה בין כלל גופי הגנת הסייבר שתאפשר את מתן המענה המתאים ביותר לסוגי האיומים השונים.

4. הוועדה סבורה, כי **רשות הסייבר הלאומית צריכה להיות הגורם האחראי על הגנת הסייבר במדינת ישראל**. באחריותה יהיו **חיזוק החוסן המדינתי, הכוונה איסופית לצורכי הגנה בסייבר וניהול ותכלול התמודדות עם אירועי תקיפה על יעדים ישראליים**, כולל אירועים בעלי אופי ביטחוני.

5. **הוועדה סבורה שאין להפוך את הרשות לסוכנות איסוף מודיעין נוספת** כדי למנוע פגיעה בפרט, שכפול יכולות יקרות במשאבי כוח אדם ובכסף, וערעור סדרי העבודה והאיזונים הקיימים בתוך קהילת המודיעין.

6. **הוועדה לא השתכנעה בצורך בקיומן של שתי יחידות סמך עצמאיות במשרד ראש הממשלה העוסקות בתחום הסייבר - מטה הסייבר הלאומי ורשות הסייבר הלאומית - המהוות יחדיו את מערך הסייבר הלאומי**. תהליכי העבודה, כפי שהוצגו לוועדה, **מייתרים הלכה למעשה את משמעות כפיפותו של ראש הרשות לראש המערך**.

7. הוועדה מייחסת חשיבות לעשייתו ולתרומתו של **מטה הסייבר** שפועל כמשימה מרכזית להפיכתה של ישראל למדינה מובילה בתחום ההגנה בסייבר. יחד עם זאת, **הוועדה סבורה שיש לבחון את מיקומו הנכון של המטה. הוועדה מסמנת את הנושא לבחינה ולמעקב בהמשך עבודתה.**

8. לנוכח עוצמת האיום שמייצר ממד הסייבר והניסיון המועט באופן יחסי בהתמודדות איתו, הוועדה ממליצה לשוב ולבחון בשנים הקרובות את ההסדרה באופן עתי על בסיס ניסיון מצטבר, במטרה לוודא שמתכונת הפעולה שנבחרה מאפשרת לעמוד ביעד של הגנת הסייבר במדינת ישראל.

רקע

9. בשנים האחרונות הולך ומתעצם איום התקיפה בסייבר. הניסיון המבצעי למול איומים אלה, מתחיל להצטבר על בסיס אירועים בהם הותקפו מערכות מחשב ישראליות, ועל בסיס לקחים מזירות רחוקות עליהן ישראל משקיפה מן הצד.

10. כפועל יוצא, מדינת ישראל וגופי הגנת הסייבר בתוכה, נמצאים עדיין בשלב מוקדם באופן יחסי של התארגנות, בהתאם להבנה של המענה הנדרש לאיום המתגבר. בין נקודות הציון הבולטות בהקשר זה ניתן למנות את ההחלטה מ-2011 על הקמת מטה הסייבר הלאומי; ואת הקמת חטיבת ההגנה בסייבר באגף התקשוב, לצד תהליכי ההקמה של זרוע הסייבר בצה"ל.

11. לאחר שהוגשו עבודות מטה שבחנו את אופן ההסדרה הלאומית הרצויה, קיבלה הממשלה החלטה להקים רשות לאומית להגנת הסייבר (החלטת ממשלה 2444 מ-15 בפברואר 2015), שבאופן רשמי החלה לפעול ב-3 באפריל 2016. במקביל מנסח המטה הלאומי את תזכיר חוק הגנת הסייבר.

12. הקמת הרשות באה למלא חלל באזורים שלא טופלו עד היום (בעיקר במרחב האזרחי) ולשפר את התיאום בין כלל גורמי הגנת הסייבר. הגם שההחלטה קבעה שלא תהיה פגיעה באחריותו ובסמכויותיו של שב"כ, הרי שמטבע הדברים, כניסתה של הרשות כשחקן חדש ומוביל "נוגסת" בתחומי האחריות והסמכות של שב"כ ומחייבת הסדרה, הן מערכתית והן מול כל אחד מגופי ההגנה בנפרד.

13. מעבר ל"חוסר הנוחות" הבין-ארגונית שהמהלך מייצר, הוא מעורר מספר שאלות עקרוניות - מהי חלוקת האחריות האופטימלית בין כלל הגופים העוסקים בהגנת הסייבר? אילו סמכויות, כלים ויכולות יש להעניק לרשות החדשה כדי לממש את אחריותה? אילו סמכויות וכלים יש לקחת - אם בכלל - מן הגופים האחרים, ומהן ההשלכות שיהיו לכך על ייעודם? האם חלוקת האחריות שתיקבע נשארת בעינה או משתנה במעבר משגרה לחירום?

14. ועדת המשנה של ועדת החוץ והביטחון לנושא ההגנה בסייבר, בראשות חה"כ אבי דיכטר[1] **(להלן הוועדה)**, ניהלה בשנה האחרונה שורה של דיונים וביקורים (לפירוט ראה נספח) כדי ללמוד ולפקח על אופן ההיערכות המדינתית להגנת הסייבר, ולבחון את משמעויות החלטת הממשלה על הקמת הרשות הלאומית ואופן מימושה.[2]

15. במהלך עבודתה נחשפה הוועדה להשקפות עולם שונות ביחס לאיום הסייבר ולאסטרטגיית ההגנה המתאימה, כמו גם למאבקי כוח והיעדר שיתוף פעולה. בעוד שהוועדה רואה בוויכוח לגבי תפיסת האיום דיון מפרה שיש להמשיך ולקיימו, הרי שהיעדר שיתוף פעולה ואף "החרמות" הדדיות נתפסו על ידה בחומרה, והוועדה התייחסה לכך בדיוניה. **בהקשר זה, הוועדה רואה בחיוב את השינוי**

---

[1] חה"כ דיכטר מונה ב-31 במאי 2016 ליו"ר ועדת החוץ והביטחון ולראשות ועדת המשנה להגנה בסייבר מונתה חה"כ ענת ברקו.

[2] סוגיית הסייבר מטופלת במשך שנים גם בוועדת המדע והטכנולוגיה של הכנסת, ששמה את עיקר הדגש לנושא השקעת המדינה בפיתוח הידע בנושא, ובמוכנות הגופים האזרחיים לאירוע של תקיפת סייבר.

בגישה בתקופה האחרונה שהוביל לגיבוש מסמך הבנות בין רשות הסייבר הלאומית והשב"כ, שנחתם ב-9 ביוני 2016.

16. מטרת הדו"ח, לבחון את חלוקת האחריות והסמכויות הרצויה בין כלל גופי הגנת הסייבר שתאפשר את מתן המענה המתאים ביותר לסוגי האיומים השונים (בקשת האיומים שבין פלילי לביטחוני, ובין אירוע תודעתי לאירוע של הקרסת מערכות). הדו"ח מציג את הבנות הוועדה לגבי חלוקת האחריות הרצויה, תוך הבעת עמדתה לגבי מהלכים נדרשים או כאלה שיש להימנע מהם בסוגיות אותן היא רואה כקריטיות בהמשך התהליך.[3]

17. בנוסף, מתוך הבנה שהמערכת נמצאת בתהליך למידה, המסמך מציף סוגיות המחייבות, לדעת הוועדה, המשך בחינה ודיון ללא קביעת עמדה חלוטה לגביהן בשלב זה.

החלטות הממשלה בנושא הגנת הסייבר

18. בשנים האחרונות קיבלו ממשלות ישראל מספר החלטות שנועדו לקדם את היכולת הלאומית במרחב הסייבר ואת ההיערכות הלאומית להגנה, והן:

א. החלטה מספר 3611 מיום 7 בפברואר 2011 בנושא קידום היכולת הלאומית במרחב הקיברנטי - במרכזה, ההחלטה להקים מטה קיברנטי לאומי במשרד ראש הממשלה (ב-2015 שונה שמו למטה הסייבר הלאומי), להסדיר את האחריות לטיפול בתחום הקיברנטי (באמצעות הצעה לתפיסת הגנה כוללת על המרחב הקיברנטי שיגיש המטה לממשלה) ולקדם את יכולת ההגנה במרחב הקיברנטי.

ב. החלטה מספר 2443 מיום 15 בפברואר 2015 בנושא קידום אסדרה (רגולציה) לאומית והובלה ממשלתית בהגנה בסייבר - במרכזה הטלת האחריות על הרשות הלאומית להגנת הסייבר שתקום להוביל את נושא הרגולציה במגזר האזרחי, ולהקים יחידה להגנת הסייבר בממשלה (יה"ב) שתיתן הנחיה מקצועית למשרדי הממשלה.

ג. החלטה מספר 2444 מיום 15 בפברואר 2015 בנושא קידום ההיערכות הלאומית להגנת הסייבר - במרכזה ההחלטה להקים רשות לאומית להגנת הסייבר במתווה תלת-שנתי (2015-2017) כגוף בעל מאפיינים אזרחיים וביטחוניים-אופרטיביים, ולגבש מתווה להעברת האחריות להנחיית מערכות ממוחשבות חיוניות משב"כ לרשות.

---

[3] הוועדה פרסמה טיוטה לדו"ח וקיבלה מהגופים השונים התייחסות כתובה ובעל-פה במסגרת דיון שהוקדש לכך, ועדכנה את מסריה בדו"ח זה.

עקרונות לחלוקת האחריות בין גופי הגנת הסייבר במדינה

19. בבואה להצביע על עמדתה באשר לחלוקת האחריות והסמכות, לבניין הכוח ולהגדרת המשימות של גופי ההגנה השונים, התייחסה הוועדה למתחים ולהנחות היסוד הבאים:

א. המתח בין תפיסות עולם שונות - תפיסת הסייבר כאירוע בפני עצמו המחייבת, לכאורה, הובלה של גוף שכל עיסוקו בסייבר (הרשות) ומנגד תפיסתו כממד לחימה נוסף (לצד היבשה, האוויר והים) ודרך פעולה חדשה לביצוע פעולות עויינות מן הסוג הישן (כמו ריגול וטרור) המעניקה יתרון לגופי הביטחון.

ב. אף לא אחד מהגופים נהנה מיתרון מובהק, אך יש לנצל את היתרונות היחסיים של כל גוף.

ג. מניעת קווי תפר - חלל של אזורים חסרי הגנה או חוסר בהירות לגבי הנושא באחריות.

ד. קביעת תחומי החפיפה שיצמצמו את הנזק הפוטנציאלי הטמון בתפרים, אך מניעת כפילויות מוגזמות להן עלות משאבית כבדה בתקציב ובכוח אדם סייבר המצוי במחסור משמעותי כבר היום.

ה. ההכרח בשיתוף פעולה ותיאום בין כלל גורמי ההגנה.

ו. יכולת למעבר מהיר בין תרחישים שונים.

ז. שמירה על זכויות האזרח.

המלצות וסוגיות להמשך מעקב

20. איום התקיפה בסייבר מהווה אתגר גובר למדינת ישראל המחייב התארגנות משופרת מזו הקיימת כיום במרחב האזרחי והביטחוני. הוועדה גורסת כי **הממשלה וגופי הביטחון הכפופים לה זיהו היטב ובזמן את האתגר, ומקיימים צעדים חשובים לגיבוש מענה התואם את עוצמת האיום.**

21. הוועדה רואה חשיבות רבה בהקמת רשות הסייבר הלאומית, בראש ובראשונה לנוכח העובדה שהיה חסר עד כה גורם המופקד על חיזוק החוסן המדינתי בתחום הסייבר שימלא גם חלל שהיה עד כה בכל הקשור להגנה על המגזר האזרחי-כלכלי (למעט גופי התמ"ק שהונחו על-ידי שב"כ). זאת במקביל לצורך לחבר נכון וחכם בין הידע והניסיון מהתחום הביטחוני עם האזרחי והכלכלי.

22. חשיבות העניין, בהכרח לחזק את התווך האזרחי, והצורך למנוע פגיעה במגזר העסקי (פשעי סייבר, ריגול תעשייתי[4]) שעלולות להיות לה השלכות חמורות בהקשרים שונים (פגיעה כספית באזרחים רבים, הדלפת פרטים אישיים, פגיעה בחברות מפתח במשק ועוד) או הישגים מורליים בעקבות תקיפות לצורכי תודעה.

---

[4] יש לתת את הדעת באשר לריגול התעשייתי שכיום אין גורם האחראי לגביו.

23. ביחס לחלוקת האחריות, הדילמות שמייצרת הקמת הרשות הן מורכבות וממשיות. גם אם בוויכוחים ובמאבקי הכוח שהתעוררו השתלבו ענייני יוקרה ואגו, לדעת הוועדה לב הוויכוח הוא ענייני ותפיסתי ביחס למענה המתאים.

24. הוועדה סבורה, כי **רשות הסייבר הלאומית צריכה להיות הגורם האחראי על הגנת הסייבר במדינת ישראל**. באחריותה יהיו **חיזוק החוסן המדינתי, הכוונה איסופית, ניהול ותכלול התמודדות עם אירועי תקיפה על יעדים ישראליים**, כולל אירועים בעלי אופי ביטחוני.

25. הגופים הביטחוניים (צה"ל, שב"כ, מוסד) ומונחי מלמ"ב ימשיכו להיות אחראים להגנתם בהתאם למצב כיום, ויובילו את הפעילות האיסופית ובעלת המאפיינים הביטחוניים להגנה בסייבר.

26. הרשות תהנה מנגישות לכלל המידע המודיעיני (בהתאם להגדרות של ביטחון מידע) ותכיר את השיקולים השונים של הגופים הביטחוניים. **יש לוודא, כי מאחר שמדובר בגוף שעובד בממשק הדוק עם קהילת המודיעין, ייקבע לעובדיו מדרג סיווגים התואם את סוג המידע שהם נחשפים לו**.

27. הוועדה מקבלת באופן בסיסי את הטענה כי הסייבר הוא ממד פעולה נוסף המאפשר ליריב לבצע פעולות מוכרות בכלים חדשים, אולם בשל החידוש שבו, **לשנים הקרובות יש לרכז את הטיפול בו בגוף שעיסוקו היחיד הוא סייבר, הלוקח בחשבון שיקולים אזרחיים-מדיניים לצד ביטחוניים, והנהנה מנגישות למגזר האזרחי, לקהילה הבין-לאומית ולמערכת הביטחונית**.

28. **בהצגת עמדה זו הוועדה רואה הטלת אחריות כבדה על הרשות - אחריות לבצע את משימותיה הישירות, אחריות וסמכות להנחות את הגופים המונחים ולהכווין את גופי הביטחון, ובסופו של דבר, אחריות לתוצאה**.

29. יחד עם זאת, **אין גוף אחד שלו היכולת הבלעדית להתמודד עם האתגר ומתחייב שיתוף פעולה הדוק בין כלל הגורמים, על יתרונותיהם היחסיים**. לרשות ישנה הסתכלות רחבה בנושא הסייבר המשקללת גם היבטים האזרחיים ולגופי הביטחון מומחיות בהיבטים הביטחוניים.

30. **בהסדרה המוצעת ישנו פתח לחילוקי דעות וקשיים בהטלת מרות**. לדעת הוועדה, במקרה של מחלוקת בין הרשות לבין הגופים הביטחוניים, **ראש הרשות צריך להיות הגורם הפוסק**, לאחר ששמע את כלל השיקולים, מתוקף היותו האחראי להגנה. יחד עם זאת, בשביל אותם מצבים בהם לא תושג הסכמה, **חייב להיקבע מנגנון ברור לניהול מחלוקות**.

31. להוציא את ראה"מ שישמש בכל מקרה פוסק אחרון, ניתן להצביע על מנגנונים נוספים לניהול מחלוקות כמו של דרג מקצועי (למשל ור"ש), מיניסטריאלי (שר לענייני מודיעין) או אחר. **הוועדה מצפה לקבל עדכון לגבי המנגנון שייקבע**.

32. **בעת מצב של מלחמה**, הוועדה רואה חשיבות בהעברת האחריות לתכלול ולניהול ההתמודדות במרחב הסייבר **לגורם שמוביל את המערכה** (צה"ל/שב"כ) בהתאם למתאר העימות, כש"פורום

ההגנה״ של הרשות ימשיך לפעול באופן שיאפשר לה להמשיך להשפיע באופן ישיר ובאמצעות נציגות במכלול המלחמתי להגנה בסייבר בהובלת צה״ל.

33. חלוקת האחריות והסמכות משפיעה על הכלים שכל גוף נדרש להחזיק לצורך מימוש אחריותו. **הוועדה סבורה שבכל מקרה, אין להפוך את הרשות לסוכנות איסוף מודיעין נוספת,** וזאת כדי למנוע פגיעה בפרט לנוכח מתן אישור לגורם נוסף לפעול בחשאי במרחב הישראלי, שכפול יכולות יקרות במשאבי כוח אדם ובכסף, וערעור סדרי העבודה והאיזונים הקיימים בתוך קהילת המודיעין.

34. הרשות תתבסס על יכולות האיסוף של גופי המודיעין הקיימים (שב״כ, אמ״ן, מוסד), לצד מידע גלוי ואחר שהיא תקבל באמצעות חוקריה ובאמצעות ה-cert הלאומי, שת״פ קש״חי וכדומה, **וכלל עיסוקיה האופרטיביים לא יחפפו לתחומי הפעולה של גופי הביטחון.**

35. **הוועדה לא השתכנעה בצורך בקיומן של שתי יחידות סמך עצמאיות במשרד ראש הממשלה העוסקות בתחום הסייבר - מטה הסייבר הלאומי ורשות הסייבר הלאומית - המהוות יחדיו את מערך הסייבר הלאומי.** זאת, מאחר שעל פי החלטות הממשלה נראה שישנם אזורי חפיפה בחלוקת הסמכויות ביניהן. בפני הוועדה הוצגה על ידי ראש מערך הסייבר (המאגד תחתיו את המטה ואת הרשות) התפיסה לפיה המטה עוסק בתכנון ארוך טווח בנושא הסייבר (מו״פ, עידוד התעשייה והאקדמיה, ועוד) ואינו ממוקד בתחום ההגנה, בעוד הרשות היא גוף הגנה אופרטיבי הפועל עצמאית בלא צורך בקבלת אישור מצד ראש המערך בניהול ההגנה.

36. תהליכי העבודה, כפי שהוצגו לוועדה, **מייתרים הלכה למעשה את משמעות כפיפותו של ראש הרשות לראש המערך.** שכן, ראש הרשות הנו עצמאי בליבת עשייתו, ההגנה בסייבר, ולא מחויב לקבל אישור מראש המערך להחלטותיו ולפעולותיו בתחום. העובדה שהוא מדווח באופן עיתי למזכ״צ ראה״מ מצביעה גם היא על כפיפותו המעשית לראה״מ.

37. באשר **למטה הסייבר**, הוועדה מברכת על עשייתו ותרומתו, כגוף שמנותק מהאירועים השוטפים, מרחיק ראות, מחובר להתפתחויות הטכנולוגיות ופועל כמשימה מרכזית להפיכתה של ישראל למעצמת סייבר. יחד עם זאת, **הוועדה סבורה שיש לבחון את מיקומו הנכון של המטה. הוועדה מסמנת את הנושא לבחינה ולמעקב בהמשך עבודתה.**

38. בהקשר המיידי, הוועדה קובעת כי נוסח חוק הסייבר המתגבש חייב להיכתב תוך שיתוף ומעורבות כלל הגורמים הרלוונטיים (במערכת הביטחונית והאזרחית). יש לוודא, כי החוק מבטיח שכניסתה של הרשות כשחקן חדש אינה פורצת את המגבלות שהוטלו עד היום על שב״כ בכל הקשור להקפדה על שמירת זכויות הפרט. ההבנה שהמציאות בעולם הסייבר דינאמית מחייבת שהחוק יהיה מודולרי, כך שניתן יהיה לעדכן אותו מעת לעת בהתאם להתפתחויות, שכעת מוקדם מדי מכדי לצפות אותן.

39. בהקשר אחר, **הוועדה התרשמה מחולשתה של המשטרה** בשל מגבלות חוקתיות והיעדר משאבים מספיקים והיא ממליצה להרחיב את הדיון בנושא, כדי למצוא את האיזון המתאים בין הצורך לצמצם פגיעה בזכויות הפרט לבין שיפור האפקטיביות של פעולתה במרחב הסייבר. על מנת לחבר

נכונה את הידע והיכולות הלאומיות עם הצורך המשטרתי להתמודד בפשעי סייבר, הוועדה סבורה שנכון יהיה לדון בנושא בוועדות הכנסת הרלוונטיות.

40. **לסיכום, בשל עוצמת האיום שמייצר ממד הסייבר והניסיון המועט באופן יחסי בהתמודדות איתו, הוועדה ממליצה לשוב ולבחון את ההסדרה באופן עתי (במהלך 5 השנים הקרובות) על בסיס לקחי אירועים וניסיון מצטבר, וזאת במטרה לוודא שאכן חלוקת האחריות ומתכונת הפעולה שנבחרה מאפשרות לעמוד ביעד העליון בתחום זה - הגנת הסייבר במדינת ישראל.**

הערה

בקרב חברי הוועדה הובעו גם התנגדויות או הסתייגויות מחלק מההמלצות המובאות בדו"ח:

א. **יו"ר ועדת המשנה (מאז ה-31 במאי 2016), חה"כ ענת ברקו**, מדגישה את הצורך להימנע מפיזור האחריות שעלול להיווצר בין הרשות לבין הגופים הביטחוניים, וסבורה שהסמכות להכריז על מעבר משגרה לחירום ולהחליט על ניהול מערכה בעלת אופי ביטחוני שמטרתה הגנה בסייבר צריכה להיות בידי גופי הביטחון ולא בידי ראש הרשות.

ב. **חה"כ אראל מרגלית** מציג עמדה שונה מזו של הוועדה. לשיטתו, נדרשת הפרדה ברורה בין המרחב האזרחי לביטחוני. הרשות תהיה אחראית למרחב האזרחי - הקמת צוותי משימה לסקטורים השונים (בנקאות, אנרגיה וכדומה) שיתנהלו באופן חצי אוטונומי (קביעת תקני הגנה באופן מוסכם עם הרשות), תיאום בין-מדינתי, חקיקה ותיאום בין המגזר האזרחי לרשויות הביטחון. את הנושא הביטחוני יוביל גורם ביטחוני (שב"כ/צה"ל) בעל אופי משימתי ומבצעי. הפרדה דומה קיימת בארה"ב בין ה-Homeland Security האחראי לתחום האזרחי ל-NSA, CIA ו-FBI, ולא ניתנת לגוף אחד אחריות בגזרתו של האחר. בעוד 3 שנים יש לבחון אם ניתן להרחיב את סמכויות הרשות.

ג. ביחס לסוגיית המנגנון לניהול מחלוקות בין הרשות לגופי הביטחון, **חה"כ עמר בר-לב** טוען, שמרגע שראש הרשות מוגדר כגורם האחראי והפוסק, אין לקבוע מעליו מנגנון שיכול לחלוק על דעתו, מלבד ראש הממשלה. לשיטתו, יצירת מנגנון כזה עלולה לפגוע בסמכותו של ראש הרשות ולעודד מצבים של אי קבלת עמדתו.

חברי ועדת המשנה להגנה בסייבר

(לפי סדר הא"ב)

חה"כ אבי דיכטר

יו"ר ועדת החוץ והביטחון

חה"כ ענת ברקו

יו"ר ועמ"ש להגנה בסייבר

חה"כ עמר בר-לב

חה"כ מחמד שי-

חה"כ עפר שלח

בדיוני ועדת המשנה להגנה בסייבר השתתפו גם ממלאי המקום, חה"כ יואב בן-צור, חה"כ אייל בן-ראובן, חה"כ שרן השכל, חה"כ אראל מרגלית, וחה"כ מיכל רוזין.

הצוות המלווה

מר שמואל לטקו

מנהל ועדת החוץ והביטחון

עו"ד גב' מירי פרנקל-שור

יועצת משפטית של ועדת החוץ והביטחון

מר כרמל גיל

ראש תחום מודיעין וסייבר

עו"ד עידו בן-יצחק

עוזר היועצת המשפטית של ועדת החוץ והביטחון
בוועדת החוץ והביטחון

גב' דנה ברק

רכזת ועדת החוץ והביטחון

נספח

דיונים ומשתתפים

תאריך הישיבה	נושא הישיבה
5 ביולי 2015	ביקור במטה הסייבר הלאומי
14 ביולי 2015	איום הסייבר על ישראל
28 באוקטובר 2015	קידום הערכות לאומית בסייבר
22 בנובמבר 2015	ביקור בחברת החשמל
26 בנובמבר 2015	ביקור בשב"כ
17 בינואר 2016	ביקור במטה/רשות הסייבר הלאומי
21 בפברואר 2016	הגנה בסייבר בצה"ל
21 בפברואר 2016	הגנה בסייבר במוסד
21 בפברואר 2016	הגנה בסייבר במשטרה
21 בפברואר 2016	הגנה בסייבר במשרד החוץ
21 בפברואר 2016	הגנה בסייבר במלמ"ב
30 במרס 2016	דיון פנימי של ועמ"ש הגנה בסייבר
5 באפריל 2016	דיון פנימי של ועמ"ש הגנה בסייבר
13 ביוני 2016	התייחסויות הגורמים לטיוטת דו"ח הוועדה
22 ביוני 2016	דיון פנימי של ועמ"ש הגנה בסייבר

מלבד דיוני הוועדה, התקיימו פגישות רבות של חברי הוועדה והצוות המקצועי עם גורמי המטה, הרשות, השב"כ והמל"ל.