התקפות סייבר על מערכת הבחירות – איך מתמודדים?

גבי וקנין | עמי וייס

בשנים האחרונות זוהו מקרי התערבות לא מעטים מצד מדינות בתהליכי הבחירות של מדינות אחרות באמצעות טכנולוגיה המבוססת על האינטרנט. תחומי הפעולה העיקריים היו תקיפה של תהליך ביצוע הבחירות, תקיפת מפלגות ושחקנים פוליטיים וניסיונות להשפיע על תודעת הבוחרים באמצעות מניפולציות ברשתות החברתיות.

המכון הישראלי לדמוקרטיה
מרכז המחקר להגנת הסייבר
CYBER SECURITY RESEARCH CENTER
מחקר מדיניות 136

טיוטה

מרכז המחקר
להגנת הסייבר

המכון הישראלי
לדמוקרטיה

מחקר מדיניות 136

התקפות סייבר על מערכת הבחירות – איך מתמודדים?

רון שמיר | אלי בכר

טיוטה

ינואר 2019

Defending Israel's Elections from Cyber-Attack – What Should be Done?
Ron Shamir | Eli Bachar

עריכת הטקסט: קרן גליקליך
עיצוב הסדרה והעטיפה: סטודיו תמר בר־דיין
ביצוע גרפי: נדב שטכמן פולישוק
הדפסה: גרפוס פרינט, ירושלים

מסת"ב: 978-965-519-248-3

המכון הישראלי לדמוקרטיה
רח' פינסקר 4, ת"ד 4702, ירושלים 9104602
טל': 02-5300888, פקס: 02-5300867
דוא"ל: orders@idi.org.il
אתר האינטרנט: www.idi.org.il

מרכז פדרמן לחקר הסייבר – תכנית משפט וסייבר, האוניברסיטה העברית בירושלים
הפקולטה למשפטים, קמפוס הר הצופים
תא 80, מיקוד 9190501
דוא"ל: hcsrcl@mail.huji.ac.il
אתר האינטרנט: https://csrcl.huji.ac.il

המכון הישראלי לדמוקרטיה

המכון הישראלי לדמוקרטיה הוא מוסד עצמאי א־מפלגתי, מחקרי ויישומי, הפועל בזירה הציבורית הישראלית בתחומי הממשל, הכלכלה והחברה. יעדיו הם חיזוק התשתית הערכית והמוסדית של ישראל כמדינה יהודית ודמוקרטית, שיפור התפקוד של מבני הממשל והמשק, גיבוש דרכים להתמודדות עם אתגרי הביטחון מתוך שמירה על הערכים הדמוקרטיים וטיפוח שותפות ומכנה משותף אזרחי בחברה הישראלית רבת הפנים.

לצורך מימוש יעדים אלו חוקרי המכון שוקדים על מחקרים המניחים תשתית רעיונית ומעשית לדמוקרטיה הישראלית. בעקבותיהם מגובשות המלצות מעשיות לשיפור התפקוד של המשטר במדינת ישראל ולטיפוח חזון ארוך טווח של תרבות דמוקרטית נכונה לחברה הישראלית ולמגוון הזהויות שבה. המכון שם לו למטרה לקדם בישראל שיח ציבורי מבוסס ידע בנושאים שעל סדר היום הלאומי, ליזום רפורמות מבניות, פוליטיות וכלכליות ולשמש גוף מייעץ למקבלי ההחלטות ולציבור הרחב.

המכון הישראלי לדמוקרטיה הוא זוכה פרס ישראל לשנת תשס"ט על מפעל חיים – תרומה מיוחדת לחברה ולמדינה.

תוכנית המחקר להגנת הסייבר, משפט וקרימינולוגיה

תוכנית משפט וסייבר פועלת כחלק ממרכז פדרמן לחקר הסייבר באוניברסיטה העברית בירושלים ומתמקדת ב־cyber security (ביטחון המרחב הקיברנטי) מפרספקטיבה משפטית וקרימינולוגית. החוקרים בתוכנית עוסקים במגוון נושאים ותחומים, בהם: רגולציה, אחריות משפטית, מניעת פשיעה, זכויות אדם ודיני מלחמה. התוכנית פועלת לייצר ידע ולכונן שיתופי פעולה בין חוקרים, ארגונים העוסקים בזכויות אדם, גופי ממשל ותעשייה. יתר על כן, כיוון שאנו מצויים בעידן של פיתוח רגולציות ומיסוד קודים להתנהגות במרחב הסייבר ואף שותפים לעיצוב הנורמות והפרקטיקות הנוהגות הללו, חוקרי התוכנית והמרכז רואים חשיבות בתרומה להתפתחותו של שיח ציבורי בנושא ביטחון המרחב הקיברנטי בצד השיח האקדמי.

הדברים המובאים במחקר מדיניות זה אינם משקפים בהכרח את עמדת המכון הישראלי לדמוקרטיה או את עמדת תוכנית המחקר להגנת הסייבר.

תוכן העניינים

תקציר

מסמך זה עוסק בסיכונים שמקורם בהתערבות או בהשפעה על תהליך הבחירות לכנסת בישראל – במובנו הרחב – באמצעות תקיפה במרחב מקוון על ידי ישות זרה, מדינתית או תת־מדינתית. סיכונים אלה ממשיים, שכן בשנים האחרונות זוהו מקרים רבים של התערבות מדינות בתהליכי הבחירות במדינות אחרות באמצעות טכנולוגיה שמבוססת על רשת האינטרנט. עבודה זו אינה עוסקת בהשפעה על תהליך הבחירות שאינה נעשית במרחב המקוון וכן בהשפעה על תהליך הבחירות על ידי שחקנים פוליטיים ישראלים, אלא אם הם פועלים באמצעות ישות זרה או שהיא מפעילה אותם במודע כדי להשפיע על הבחירות באמצעות כלי סייבר.

מטרות המסמך הן למפות ולזהות את האיומים העיקריים על תהליך הבחירות ועל אמון הציבור בתוצאותיהן, שכן אמונו של הציבור שהמנצח והמפסיד נקבעו בהליך בחירות שלא זויף ולא שובש בדרך אחרת, חיוני לקיומם של החישוקים החברתיים הבסיסיים ביותר. איומים אלה ייבחנו על רקע הסביבה הטכנולוגית, המשפטית והמוסדית בתחום הגנת תהליך הבחירות בישראל, ועל יסוד תהליך זה מוצעות המלצות המדיניות.

מקרב המדינות שבעשור האחרון זוהו ככאלה שהפעילו מבצעי השפעה על בחירות באמצעות כלי סייבר בולטת רוסיה – אם כי היא איננה היחידה – בניסיונות ההתערבות שלה במערכות בחירות למשל באוקראינה (2014),

בארצות הברית (2016), בצרפת (2017), בגרמניה (2017) ובהולנד (2017), וכן במשאלי העם בבריטניה, בהולנד, באיטליה ובספרד (2017). פעולות אלה נועדו בדרך כלל לתמוך במועמד מסוים או להחליש אחר, ואולם חלקן לפחות נועדו ליצור בחברה הרלוונטית שסעים בסוגיות מהותיות ולהחליש בה את הלכידות החברתית; לקדם מטרות אסטרטגיות כמו החלשת ברית נאט"ו; לפגוע בעקרון הציות לנורמות הבינלאומיות; וכן לפגוע באמון הציבור בתהליך הדמוקרטי.

המרחב המקוון מספק מגוון של אמצעים ושיטות להשפעה על מערכות בחירות: גנבת מידע מאישים פוליטיים והפצתו באופן ובמועד שיזיק ליריב; שיבוש מידע במערכת הבחירות – החל בשיבוש פנקס הבוחרים וכלה בשיבוש התוצאות – במטרה לערער את אמון הציבור בתוצאותיהן; מניעת שימוש במערכות – מתקפה שתכליתה פגיעה בזמינות המערכות (DDOS) במועד מתוכנן מראש, ובמקומות שבהם נהוגה הצבעה אלקטרונית גם פגיעה במכשירי ההצבעה מבוססי המחשב; ייצור והפצה של חדשות כזב (fake news) ברשתות החברתיות; שיטוי בגורמים שלישיים באמצעות התחזות ברשת כמו למשל הונאת עיתונאים; ועוד.

הניסיון המצטבר מלמד כי בכל הנוגע למרחב המקוון ניסיונות ההתערבות בתהליך הבחירות נעשים בעזרת תקיפה בשלוש זירות עיקריות: (א) תקיפת הליך ביצוע הבחירות על כל שלביו, אם בזיוף ואם בשיבוש ובמניעה של שירות; (ב) תקיפת מפלגות פוליטיות ושחקנים פוליטיים באמצעים שונים: גנבת חומר אישי ופוליטי ופרסומו בעיתוי מתאים מבחינת יעדי התקיפה, שיבוש היערכות המפלגה לבחירות ועוד; (ג) תקיפת רשתות חברתיות ואתרי חדשות כאזורים העיקריים המאפשרים להשפיע על תודעת הבוחרים באמצעות כלים מבוססי סייבר.

תקיפה מבוססת סייבר על תהליך הבחירות עשויה לכלול שימוש בכלים טכנולוגיים כגון בוטים (bots) וטכנולוגיות מבוססות נתוני עתק (Big Data); שימוש בכלי פריצה טכנולוגיים למערכות מחשב על ידי מומחי פריצה (האקינג); וכן שימוש במגיבים מקצועיים (טרולים), פלטפורמות התחזות כמו פורומים תמימים ועוד. כלים אלה שימשו למשל במבצעי השפעה להפצת מידע מטעה והבאתו לקהל גדול מאוד; בגנבת מידע והפצתו הסלקטיבית במועד המתאים להשפעה מרבית על הבחירות; במבצעי השפעה מכוונת אישית (מיקרו טרגטינג); בהשפעה דרך פגיעה בתשתיות ועוד. המשותף לכל מהלכי השפעה

אלה הוא בדרך כלל הסתרת מקור התקיפה, כך שקשה מאוד לאתר במועד מי הארגון העומד מאחוריה וליחסה לתוקף ברור ומזוהה.

מתוצאות התקפות הסייבר על מערכות הבחירות בארצות הברית ובמדינות המערב בשנים האחרונות עולה כי אף מדינה אינה יכולה להישאר שוות נפש לנוכח האיום המוחשי של התקפות סייבר על תהליך הבחירות שלה ועל אמונו של הציבור בתוצאותיהן. נדרשת אפוא שורה של פעולות, הן במישור ההגנה והן במישור ההרתעה, כדי לחזק במידה ניכרת את כושרן של הדמוקרטיות להתגונן ביעילות נגד התקפות כאלה. ואולם כאשר דמוקרטיה ליברלית מבקשת להתגונן מפני התקפות מסוג זה, עולות שאלות מושגיות ועקרוניות רבות, שהעיקרית בהן היא כיצד להבטיח שפעולות התגוננות מפני התקפות המכוונות נגד תהליך הבחירות לא יפגעו בעצמן בעקרונות הדמוקרטיה הליברלית כגון בחופש הביטוי, בפרטיות ובשוויון.

תקיפות סייבר כדרך לפגוע בתהליך הבחירות בישראל עלולות להיעשות בכל הדרכים שבהן הותקפו מערכות בחירות בארצות אחרות. בנוסף, ישראל היא חברה משוסעת ומקוטבת, שיש בה מתחים פנימיים ניכרים בשאלות רבות: יחסי יהודים־ערבים, דת ומדינה, עתיד השטחים ועוד. לפיכך לפגיעה בהסכמה החברתית על מנגנון הבחירות כמופע הדמוקרטי העיקרי וכמקור ללגיטימציה של השלטון – וכן לכרסום באמונו של הציבור בתוצאות הבחירות – עלולה להיות השפעה הרסנית במיוחד על החישוקים החברתיים המאפשרים את ניהול המחלוקות החברתיות בחברה מתפקדת, ומכאן החשיבות המיוחדת שבהגנה על תהליך הבחירות בישראל.

מבדיקת המבנה המוסדי של הארגונים האחראים על חלקים הנוגעים לאבטחת מערכת הבחירות, במובנה הרחב, מפני התקפות סייבר, עולה כי אחריות זו מתחלקת – בעניינים המפורטים במסמך – בין גורמים אחדים, לרבות ועדת הבחירות המרכזית, מערך הסייבר הלאומי, שירות הביטחון הכללי, משטרת ישראל, קצין הכנסת, משרד הפנים, הרשות להגנת הפרטיות ורשם מאגרי המידע ויחידת הסייבר בפרקליטות המדינה.

נראה כי על הגנת ביצוע הבחירות מפני תקיפות סייבר מופקדת ככלל ועדת הבחירות המרכזית, כשעל החלק המקדים (הכנת פנקס הבוחרים) מופקד משרד הפנים. לא ברור מי הגורם האחראי על הגנתן של המפלגות, ובפועל עניין

זה נמצא בטיפול המנכ"לים שלהן. בכל הנוגע לשחקנים הפוליטיים העשויים לשמש יעד לתקיפה, קצין הכנסת אחראי באופן חלקי על אבטחת המידע של חברי הכנסת המכהנים ועוזריהם הפרלמנטרים, אבל לא ברור מי מופקד על הגנה מפני התקפות סייבר של אישים פוליטיים שאינם חברי כנסת. התחום של השפעה באמצעות מניפולציה ברשתות חברתיות ואתרי חדשות הוא הבעייתי ביותר להגדרה ולתיחום אחריות, ובעניין זה יש לבחון את תיחום האחריות בין מערך הסייבר הלאומי לשירות הביטחון הכללי.

הבעיה העיקרית מקורה בעובדה שניטור הרשת כדי להגן על בחירות חופשיות ודמוקרטיות היא דרך פעולה בעלת סיכונים ניכרים בדמוקרטיה, שכן קיים חשש שמעקב אחר פעילות הבוחרים, התעמולה ופעולתם של פעילים פוליטיים, תיצור אפקט מצנן על חופש הביטוי ותפגע בפרטיות ובשוויון בבחירות – אינטרסים שמצויים בליבת ההליך הדמוקרטי. נובע מכך כי התנאי המוקדם לכל אסדרה (רגולציה) או חקיקה בנושא חייב להיות הערכת השפעתה על חופש הביטוי, על הגנת הפרטיות ועל זכויות אזרח אחרות, לנוכח הרגישות המיוחדת של תהליך הבחירות.

זאת ועוד, הרגישות היתרה של תהליך הבחירות מחייבת קיום כללי כפיפות וכללי דיווח ייחודיים, בעיקר בכל הנוגע ליחס בין האחריות החוקתית של ועדת הבחירות המרכזית על טוהר הבחירות במובנו הרחב, ובין כפיפותם של ארגוני הביטחון למרות הממשלה. עוד נדרש לקבוע את עקרונות התיאום והתיחום בעניין זה בין גורמי הביטחון והאכיפה עצמם, את העקרונות ליידוע הציבור ועוד.

המלצות המדיניות שלהלן נועדו לחזק ולשפר את ההגנה על תהליך הבחירות בישראל, במובנו הרחב, מפני התקפות במרחב המקוון על ידי ישויות זרות, הן כדי למנוע השפעה על תוצאות הבחירות והן כדי לשמור על אמון הציבור בתוצאותיהן.

עיקר ההמלצות הן:

(1) מוצע לקבוע שהאחריות הכוללת על הגנת תהליך הבחירות מפני התערבות של ישות זרה תוטל על ועדת הבחירות המרכזית, מתוך קביעה מפורשת כי העצמאות החוקתית והמוסדית של ועדת הבחירות המרכזית תישמר גם בתחום

זה. כנגזרת מכך יש לקבוע את אחריותו ואת סמכויותיו של יושב ראש ועדת הבחירות המרכזית בתחום זה.

(2) מוצע לכונן ועדה מייעצת קבועה ליושב ראש ועדת הבחירות המרכזית לעניין הגנת תהליך הבחירות מפני התקפות סייבר שמקורן בישות מדינתית זרה, שתפקידיה יהיו בין היתר לרכז ולשתף את המידע בין הגופים בנוגע להתקפות סייבר נגד תהליך הבחירות; להמליץ ליושב ראש ועדת הבחירות המרכזית על דרכי הפעולה לאיתור תקיפה כאמור, להצביע על הגורם האחראי לה ועל הדרך לסיכולה או לצמצום פגיעתה, ולהמליץ ליושב ראש ועדת הבחירות המרכזית המלצות לעניין פרסום המידע לציבור, כולו או חלקו, לרבות לעניין המועד לכך.

(3) מוצע להכריז על תהליך הבחירות בתור "תשתית לאומית קריטית", ולעגנו בחוק הבחירות לכנסת.

(4) מוצע לקבוע שהמטה לביטחון לאומי (מל"ל) יגבש תפיסה כוללת להגנה על מערכת הבחירות בישראל מפני התערבות זרה ויביאה לאישור הגורמים המוסמכים – הממשלה או הקבינט.

(5) מוצע להסדיר את אחריות ההגנה על המפלגות הפוליטיות מפני התקפות סייבר ואת אופן מימושה ומימונה, לרבות בדרך של הקצאת "תקציב צבוע" בתקציב הבחירות של המפלגות כדי שיוכלו לממש את המלצות האבטחה באופן אוטונומי.

(6) מוצע להטיל את האחריות להגנה על חברי כנסת ועל עוזריהם הפרלמנטרים על קצין הכנסת, ולעגן כללי דיווח בין הגורמים הקשורים להגנת תהליך הבחירות בדבר כל חשד לתקיפת סייבר של חברי כנסת או עוזריהם הפרלמנטרים.

(7) מוצע להטיל את האחריות להגנה על שימושי מחשב של חברי כנסת שאינם באחריות קצין הכנסת, וכן את ההגנה מפני תקיפות סייבר על אישים פוליטיים שאינם חברי כנסת על מנכ"לי המפלגות על פי כללי אבטחת מידע שתעביר אליהם ועדת הבחירות המרכזית בהתאם להמלצות שיתקבלו ממערך הסייבר הלאומי.

(8) מוצע לקבוע, בהמלצה או בהוראת חוק מחייבת, שהבחירות המקדימות במפלגות יתבצעו בפתקי הצבעה ולא במערכת ממוחשבת.

(9) מוצע לקבוע כי הגורם האחראי להגנה מפני פעולות השפעה מבוססות סייבר ברשתות חברתיות ובאתרי חדשות יהיה מערך הסייבר הלאומי. אם יתגלה מהלך כזה, ידווח עליו ליושב ראש ועדת הבחירות המרכזית ולשירות הביטחון הכללי. הסדרים לעניין האחריות לטיפול בתקיפה כזאת ולסיכולה ייקבעו בין מערך הסייבר הלאומי לשירות הביטחון הכללי בהנחיית יושב ראש ועדת הבחירות המרכזית. לנוכח רגישות הנושא, מוצע כי תוקם לעניין זה יחידה ייעודית שתהיה חלק ממערך הסייבר הלאומי, ועליה יפקח גוף שבראשו שופט בדימוס. גוף זה יבטיח שמשימות היחידה יוגבלו לזיהוי שימוש ברשתות החברתיות במטרה להשפיע על תהליך הבחירות בישראל למען אינטרסים זרים.

(10) מוצע לקבוע כי הפרסום ברבים של חשיפת מבצע השפעה שארגנה ישות זרה יהיה בסמכותו של יושב ראש ועדת הבחירות המרכזית ובכפוף להחלטתו.

(11) מוצע להגיע להסדרי שיתוף פעולה בינלאומיים לאיתור מקור תקיפה שזוהתה לרבות בדרך של אמנה בין־מדינתית.

(12) מוצע לקבוע אמנה שבה יתחייבו המפלגות להימנע מהפעלת חשבונות וירטואליים (בוטים וטרולים) כחלק מקמפיין פוליטי, ישירות או בעקיפין

(13) מוצע לקבוע איסור פלילי מפורש על קנוניה חשאית (collusion) בין אזרח או תושב ישראל ובין ישות זרה במטרה להשפיע על הבחירות. יש לנסח את האיסור באופן מצומצם וחד כך שלא יפגע בפעילות ראויה שאין כוונה להגבילה.

(14) מוצע לעודד את הקמתה של מערכת אזרחית רחבה לניטור ולבדיקה של עובדות, כחלק ממנגנון החיסון הציבורי נגד הטיה מכוונת.

(15) מוצע לבחון את האפשרות לחקוק חוק האוסר על שימוש במידע אישי לשם מיקרו־טרגטינג פוליטי, או לכל הפחות לחייב שקיפות ברורה של הנמענים שמדובר בהודעה פוליטית.

ביישום המלצות אלה ובהמשך המעקב המוסדי אחרי השינויים הטכנולוגיים וההתפתחויות בתחום התקיפה המבוססת סייבר יש כדי לחזק את יכולת ההגנה המדינתית וכן לעורר מודעות ציבורית לנושא, שאף היא נדבך חיוני בחוסן הדמוקרטי.

מבוא

מסמך זה עוסק בסיכונים שמקורם בהתערבות או בהשפעה על תהליך הבחירות לכנסת בישראל, במובנו הרחב, באמצעות תקיפה במרחב המקוון **המתבצעת על ידי ישות זרה**, מדינתית או תת־מדינתית. סיכונים אלה ממשיים, שכן בשנים האחרונות אירעו כמה וכמה מקרים שבהם זוהתה התערבות של מדינות בתהליכי הבחירות במדינות אחרות בעזרת טכנולוגיה המבוססת על רשת האינטרנט.

הטעמים העיקריים להתמקדות בתקיפה של תהלך הבחירות במרחב המקוון על ידי ישות זרה מקורם במאפייניה הייחודיים של התערבות זו: ראשית, משום שהיא מאפשרת להתערב מרחוק, בהיקף רחב, בעלות קטנה יחסית, באופן אפקטיבי, מתוך הסתרת זהותו של הגורם העומד מאחורי התקיפה ובמגוון שיטות ואמצעים. שנית, משום שצורת תקיפה זו לא רק מנסה לפגוע במועמד פלוני או לקדם את סיכוייו של מועמד אלמוני, אלא יש בה פוטנציאל לערער את אמונו של הציבור בשיטה עצמה; שלישית, משום שהכלים העומדים לרשות מדינות ואף ישויות תת־מדינתיות בדרך כלל רבי עוצמה מאלה העומדים לרשות השחקנים הפוליטיים בתוך המדינות עצמן; רביעית, משום שיש הבחנה עקרונית ומהותית – הנוגעת לחירויות כמו חופש הביטוי – בין הכלים שאפשר ורצוי להפעיל בהתגוננות מפני התערבות מצד ישות מדינתית זרה, ובין הכלים שנכון להפעיל כשמדובר בפעילות שהיא חלק מהמאבק הפוליטי בתוך המדינה עצמה. מכאן שיש ערך מהותי להבחנה בין סוגי התקיפות, וכאמור עניינו של מסמך זה הוא ההתקפה על תהליך הבחירות מצד ישות זרה.

עבודה זו אינה עוסקת אפוא בהשפעה על תהליך הבחירות שאינה מתבססת על המרחב המקוון וכן אינה עוסקת בהשפעה על תהליך הבחירות מצד שחקנים פוליטיים ישראלים, אלא אם הם פועלים באמצעות ישות זרה או שהיא זו שמפעילה אותם במודע לשם השפעה על הבחירות באמצעות כלי סייבר. ייתכן שיש מקום להרחיב את היריעה גם לתחומים אלה, ואולם הם חורגים מהיקפה של עבודה זו.

לתקיפות ולניסיונות ההשפעה של ישות זרה דרך המרחב המקוון חשיבות ציבורית גדולה ביותר, שכן אמונו של הציבור בהליכי בחירת השלטון ובאפשרות להחליפו ניצב בליבה של הדמוקרטיה, והוא הבסיס לקיומם של החישוקים החברתיים הבסיסיים ביותר. מטרות המחקר שלנו אפוא למפות ולזהות את האיומים העיקריים הן על תהליך הבחירות במדינות דמוקרטיות והן על אמון

הציבור בתוצאותיהן הנשקפים מתקיפות סייבר מצד ישויות זרות; לנתח את זירות ההשפעה האפשריות בישראל; לסקור את הסביבה הטכנולוגית, המשפטית והמוסדית שאמונה על הגנת תהליך הבחירות בישראל; ולהמליץ על פעולות שיש לנקוט להקטנת האיום. המסמך אינו עוסק אפוא לא בהשפעה על תהליך הבחירות שאינה נעשית במרחב המקוון, ולא בהשפעה על תהליך הבחירות של פעולות שנוקטים שחקנים פוליטיים ישראלים במרחב המקוון, אלא אם הם פועלים באמצעות ישות זרה או שהיא זו שמפעילה אותם. ייתכן שיש מקום להרחיב את היריעה גם לתחומים אלה, אבל הם חורגים מהיקפו של מחקר זה.

במסמך ייעשה שימוש במונחים האלה:

- **תהליך הבחירות.** כלל הפעולות הקשורות לבחירות לכנסת לרבות התהליכים הקשורים לביצוע הבחירות עצמן (ע"ע); לפעולות שנוקטים אישים פוליטיים ומפלגות פוליטיות; וכן לפעולות בנושא הבחירות המתבצעות ברשתות חברתיות ובאתרי החדשות המקוונים.
- **ביצוע הבחירות.** כלל הפעולות והמהלכים הנוגעים למימוש בפועל של הבחירות, החל בהכנת ספר הבוחרים וכלה בפרסום תוצאות הבחירות לכנסת.
- **סייבר/ סייברספייס/ מרחב קיברנטי/ מרחב מקוון.** מונחים חליפיים בעלי משמעות דומה. במסמך זה שם כולל למערכות מחשב, רשתות מחשבים ותקשורת בין מחשבים, לרבות האינטרנט עצמו.
- **התקפת סייבר.** לעניין מסמך זה כל פעילות במרחב המקוון כגון שיבוש, חבלה, גנבת מידע או השפעה על משתמשי האינטרנט שמטרתה להשפיע על הדמוקרטיה בכלל ועל מערכת הבחירות בפרט. דוגמאות: החדרת וירוס למחשבי שחקן במערכת הבחירות, מבצע השפעה (ע"ע) ברשתות החברתיות באמצעות טרולים[1] ועוד.
- **ישות זרה.** מדינה זרה שאינה עוינת בהכרח, לרבות ארגונים מדינתיים וארגונים אחרים (ארגוני טרור, ארגוני פשיעה וכיו"ב) שפועלים מחוץ לישראל, בין שהם משתפים פעולה עם מדינות או עם ארגונים מדינתיים ובין שלא.

1 מגיבים מקצועיים בשכר, ראו הגדרה **להלן**, בחת־פרק א2.

• **מבצע השפעה מבוסס סייבר.** למונח זה הגדרות שונות.[2] ההגדרה למסמך זה: מהלך מתואם המתבסס על הפעלת יכולות מדינתיות במרחב המקוון לשם קידום מהלכים או שינוי עמדות ותפיסות של מדינה־יריבה במטרה לקדם את האינטרסים של הגורם המפעיל את המבצע.

פרק א סוקר את הניסיון שהצטבר במדינות אחרות בכל הנוגע לניסיונות ההשפעה של מדינות זרות באמצעות התקפות סייבר, שממנו אפשר ללמוד מהם האיומים העיקריים גם על תהליך הבחירות בישראל. אין סיבה להניח כי מדינת ישראל חסינה מפני התערבות כזאת. **פרק ב** סוקר את שלוש הזירות הרלוונטיות לתקיפה של תהליך הבחירות בישראל ולהשפעה על התוצאות הסופיות: ביצוע הבחירות בפועל; השחקנים הפוליטיים העיקריים (מפלגות ואישים פוליטיים); וזירת הרשתות החברתיות ואתרי החדשות, שמניפולציה עליהם עשויה להשפיע על דעת הקהל. **פרק ג** מתמקד במיפוי המוסדי והמשפטי של הרשויות הרלוונטיות שמתפקידן לבצע את הבחירות בישראל ולהגן על תהליך הבחירות, במובנו הרחב, מפני תקיפה מבוססת סייבר של ישות זרה. מתוך מיפוי זה אפשר להסיק מהם התחומים העיקריים שיש לחזק. **פרק ד** מתווה המלצות מדיניות, לרבות הצעות לתיקוני חקיקה ולשינויים מוסדיים כדי לשפר את ההגנה מפני תקיפה מבוססת סייבר שמבצעת ישות זרה במטרה להשפיע על תהליך הבחירות בישראל.

2 ראו למשל את ההגדרה של מכון RAND המופיעה אצל Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, & Lowell H. Schwartz, Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities (2009):

> Influence operations are the coordinated, integrated, and synchronized application of national diplomatic, informational, military economic, and other capabilities in peacetime, crisis, conflict, and postconflict to foster attitudes, behaviors, or decisions by foreign target audiences that further U.S. interests and objectives.

חלק א

בחינת "איום הייחוס": סקירת סוגי ההתערבות של מדינות וישויות זרות בהליכי בחירות במדינות אחרות

במטרה ללמוד מניסיונן של מדינות אחרות מהם האיומים העיקריים על תהליך הבחירות ועל אמון הציבור בתוצאותיהן בהקשר של תקיפות סייבר מצד ישויות זרות, נבחן שלושה היבטים:

(**1**) מיהם הגורמים העיקריים העלולים לסכן את תהליך הבחירות בדמוקרטיות המערביות?

(**2**) מהם האיומים העיקריים על התהליך וכיצד בוצעו התקיפות במקרים שנבחנו?

(**3**) אילו דרכי התגוננות נקטו המדינות?

התשובה לשאלה מהי התערבות בבחירות איננה חד־משמעית, שכן מעצם טבעה היא קשורה למתחים הפוליטיים המצויים ממילא בין המפלגות והמועמדים היריבים. מכאן שעצם היכולת להגיע למסקנה מוסכמת בנוגע לקיומה ולטיבה של ההתערבות, יעדיה והאפקטיביות שלה אינה עניין פשוט. כך למשל אף ששאלת התערבותה של רוסיה בבחירות 2016 בארצות הברית, יעדיה ושיתוף הפעולה האפשרי שלה עם מנהלי מסע הבחירות של דונלד טראמפ מעסיקה רשויות מודיעין ומשפט בארצות הברית (כמו שיתואר להלן), אמינות הבדיקות והחקירות עצמן נמצאות בצל המחלוקת הפוליטית החריפה בין המפלגה הדמוקרטית לרפובליקאית.

מסיבה זו לא הצליחה ועדת המודיעין של הקונגרס (House Permanent Select Committee on Intelligence) להגיע לידי הסכמה בנוגע למעורבותה של רוסיה בבחירות 2016[3] בעיקר בשאלת שיתוף הפעולה של מטה טראמפ עם הרוסים, ולצד פרסום דעת הרוב הרפובליקאי, פרסמו חברי הוועדה הדמוקרטים

3 House Permanent Select Committee on Intelligence, *Report on Russian Active Measures* (March 2, 2018)

דו"ח משלהם.[4] במאי 2018 לעומת זה פרסמה ועדת המודיעין של הסנאט (The Senate Select Committee on Intelligence) דין וחשבון חלקי,[5] שבעיקרו של דבר מאמץ את מסקנות הדוח של קהילת המודיעין, המייחסת לרוסיה התערבות בבחירות 2016 נגד הילרי קלינטון ולטובת דונלד טראמפ (ראו להלן). המשך החקירה של אותה ועדה וחקירות נוספות כגון זו של ועדת המשפט של הקונגרס (House Judiciary Committee) וכמובן חקירתו של התובע המיוחד רוברט מולר ממשיכות להתנהל בעת כתיבת שורות אלה, ובהן נבדקים בין השאר החשדות שצוות מסע הבחירות של הנשיא טראמפ שיתף פעולה עם הרוסים. כל אותה העת עצם קיומן ואמינותן של החקירות מצוי בעימות פוליטי וציבורי חריף.

כך או כך המידע שהצטבר בשנים האחרונות בדבר התערבות באמצעות כלי סייבר במערכות בחירות של מדינות אחרות – בדגש על ההתערבות הרוסית – מאפשר לשרטט את מגוון האמצעים והשיטות שנעשה בהן שימוש, להבין על בסיס ניתוח זה את מפת האיומים על תהליך הבחירות בדמוקרטיה, ומכאן גם להמליץ על האסטרטגיה ועל הכלים שעל דמוקרטיה לנקוט נגד התקפות אלה.

.1
מיהו התוקף ומהן מטרות התקיפה?

ניסיונות של מדינות להשפיע על תוצאות של מסעות בחירות פוליטיים במדינות אחרות, לפגוע במועמדים או במפלגות ולחזק מועמדים או מפלגות לטובת אינטרסים של המדינה־המתערבת או לשם פגיעה באמון הציבור בשיטה הפוליטית הנוהגת ובתוצאותיה, אינם עניין חדש. בשנות החמישים של המאה

4 לדוח של דעת המיעוט ראו House Permanent Select Committee on Intelligence, *Minority Views* (March 2, 2018)

5 *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations* (May 8, 2018)

ה־20, בעיקר בתקופת המלחמה הקרה, התערבו הן ברית המועצות והן ארצות הברית עצמה באופן חשאי ובגלוי בקמפיינים פוליטיים במדינות רבות בעיקר במרכז אמריקה ובדרומה וכן באפריקה ובאיראן, בניסיון להטות את הבחירות למועמד שלטובתו כוונה ההתערבות.[6]

הייחודיות שבהתערבות במערכות פוליטיות באמצעות תקיפות מבוססות סייבר וההבדל בינן ובין "מבצעי השפעה" קלסיים הם במגוון האמצעים העומדים לרשות התוקף וביכולתו לבצע תקיפה רחבת היקף ולהגיע לקהלים גדולים בזכות יכולות טכנולוגיות מתקדמות.[7] הממד הטכנולוגי כולל בעיקר יכולות פריצה (hacking) לשם גנבת מידע, שיבוש או זיוף של תהליך הבחירות – במובנו הרחב (כולל באמצעות תקיפה של מפלגות ושחקנים פוליטיים רלוונטיים אחרים כמו חברי פרלמנט, עוזרים וחברות ייעוץ ותמיכה הקשורות לקמפיינים הפוליטיים), וכן הפעלת יכולות כגון רובוטים המתחזים למשתמשים לגיטימיים ברשת (בוטים, bots) לשם שימוש מניפולטיבי ברשתות חברתיות כדרך להשגת השפעה פוליטית.[8] בהקשר זה מעניין לציין את חשיפתו של רן בר־זיק מעיתון "הארץ"[9] על רשת הבוטים הפועלת בישראל כדי להפיץ מידע כוזב, וכן את מחקרם של האקטיביסטים נעם רותם ויובל אדם, שחקרו לעומק התנהגות של רשת בוטים בישראל.[10]

אף שעולם הסייבר מספק גם לארגונים וליחידים יכולות ניכרות לתקוף ולשבש מערכות מחשב, הניסיון מלמד כי השחקניות הראשיות במתקפות הסייבר המכוונות נגד המערכת הפוליטית הן מדינות, כשארגונים מעורבים בדרך כלל

6 Dov H. Levin, *When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results*, 60 International Studies Quarterly 189–202 (2016)

7 Andy Greenberg, *Everything We Know About Russia's Election-Hacking Playbook*, Wired (September 9, 2017)

8 על בוטים ראו **להלן**, בחמ־פרק א2.

9 רן בר־זיק "מה עושה ח"כ לשעבר ברשת הבוטים שניסתה להשמיץ את ליברמן?" **הארץ** (30.11.2018).

10 נעם רותם ויובל אדם "פרויקט הבוטים הגדול – מועדון המעריצים של בנימין נתניהו" **בלוג לפני האיתחול** (6.11.2018).

כזרוע ביצוע של מדינות במטרה לטשטש את מקור התקיפה. לרוב רק למדינות יש את המשאבים הדרושים לניהול מבצע השפעה בקנה מידה גדול וכן את הרצון הפוליטי, המתורגם לכלים בעוצמה מדינתית, לפעול באופן אפקטיבי בזירה זו. ארגונים מסתפקים בדרך כלל במטרות בעלות מאפיינים עסקיים או מאפייני פשיעה, אם לצורכי תעמולה של הארגון ואם למטרות אחרות, מוגבלות הרבה יותר, אם כי אין להוציא מכלל אפשרות שארגונים בעלי גוון אידיאולוגי מובהק - כמו תנועות דתיות או מתנגדי הפלות – יפעלו כדי להשפיע על בחירות במדינות אחרות.

ברוב המקרים קשה לדעת מי בדיוק עומד מאחורי התקפת סייבר, הן בשל מאמציו של הגורם התוקף להסתתר מאחורי האנונימיות שמאפשרת רשת האינטרנט, והן בשל האפשרות לפעול בצורה מבוזרת, בזירות פעולה שונות, בגמישות תפעולית ובהיקפים רחבים. מאמצי ההסתרה מביאים לידי כך שלעיתים קרובות, גם כשהתקפת סייבר מזוהה, נדרש זמן לאתר את מקור התקיפה ולייחס אותו בבירור לגורם העומד מאחוריו. קושי זה, שאליו מתווסף הקושי בהצגת ראיות ברורות, מאפשר לתוקף להכחיש לא פעם את מעורבותו.

אף שבעשור האחרון זוהה שמדינות אחדות – בין היתר קוריאה הצפונית ואיראן – ניסו להשפיע על בחירות במדינות אחרות באמצעות מבצעי תקיפה בכלי סייבר, מעמדה המיוחד של רוסיה בתחום זה הוא כמעט מוסכמה.[11] כך למשל בשנים האחרונות נטען, עם ראיות לא מעטות, שארגוני המודיעין של רוסיה, לעיתים בשיתוף עם קבוצות האקרים המוכרות ככאלה שפועלות בהכוונת המודיעין הרוסי (GRU), התערבו בין היתר במערכת הבחירות באוקראינה (2014), בארצות הברית (2016), בצרפת (2017) בהולנד (2017)[12] ובגרמניה (2017),[13] וכן

11 Lucan Ahmad Way & Adam Casey, *Russia Has Been Meddling in Foreign Elections for Decades – Has It Made a Difference?*, Washington Post (January 8, 2018)

12 ראו בדוח שירותי המודיעין של הולנד: AIVD, Annual Report Review 9 (2017). זמין בקישור: https://tinyurl.com/ybrwgwted

13 Constanze Stelzenmüller, *The Impact of Russian Interference on Germany's 2017 Elections* (Testimony before the U.S. Senate Select Committee on Intelligence June 28, 2017) זמין בקישור: https://tinyurl.com/ycx4fent

במשאלי העם בבריטניה,[14] בהולנד, באיטליה ובספרד (2017).[15] שיטות הפעולה כללו בין היתר מבצעי השפעה של מידע מטעה (דיסאינפורמציה); התקפות סייבר שנועדו להזיק לתהליך הבחירות, לשבש או לזייף אותו; טיפוח בעלי ברית; והסתייעות בגורמים אחרים כמו אתרי הדלפות וקבוצות האקרים פרטיות. בדרך כלל נועדו פעולות אלה לתמוך במועמד מסוים או להחליש אחר, אבל חלקם לפחות נעשו למטרות עקיפות יותר: לפצל את החברה במדינה היריבה בסוגיות מהותיות ולהחליש את הלכידות החברתית בה; לקדם מטרות אסטרטגיות כמו החלשת ברית נאט"ו;[16] לפגוע בעקרון הציות לנורמות הבינלאומיות כמו למשל האיסור על תוקפנות (כגון השתלטות רוסיה על קרים) או לפחות אי־החלתן המעשית על רוסיה;[17] ולפגוע באמון הציבור בתהליך הדמוקרטי,[18] שהוא נקודת חוזקה חשובה של יריבותיה של רוסיה.[19]

ב־6 בינואר 2017 פרסמה קהילת המודיעין האמריקאית – לשכת החקירות הפדרלית (FBI), סוכנות הביון המרכזית (CIA) והסוכנות לביטחון לאומי (NSA) – את הערכתה שרוסיה, בהוראתו האישית של נשיאה ולדימיר פוטין, התערבה במגוון אמצעים בבחירות שהתקיימו בארצות הברית בשנת 2016.[20] התערבות רוסיה בבחירות, כך לפי הדוח, נועדה לפגוע בסיכויי בחירתה של

14 Howard Kollanyi, Bots, #StrongerIn, and #Brexit: Computational Propaganda During the UK–EU Referendum (2016)

15 Joseph R. Biden Jr. & Michael Carpenter, *How to Stand Up to The Kremlin: Defending Democracy Against Its Enemies*, 97 Foreign Affairs 44–57 (2018)

16 Stelzenmüller, *The Impact*, **לעיל** ה"ש 13.

17 Mason Richey, *Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and The Strategic and Tactical Deployment of Disinformation*, 16 (1) Asia Europe Journal 101 (2018)

18 Juan C. Zarate, *The Cyber Attacks on Democracy*, 8 The Catalyst (2017)

19 Anila Polyakova & Spencer P. Boyer, *The Future of Political Warfare: Russia, The West, and The Coming Age of Global Digital Competition*, 3 (Foreign Policy at Brookings, 2018)

20 ICA, *Assessing Russian Activities and Intentions in Recent US Elections* (January 6, 2017)

מועמדת הדמוקרטים הילרי קלינטון ולקדם את בחירתו של דונלד טראמפ. הדוח קובע כי ניסיונות אלה של רוסיה כללו שורה של אמצעים, גלויים וחשאיים, בעיקר באמצעות מבצעים בתחום הסייבר, לרבות מבצעי השפעה על התודעה שבוצעו דרך רשתות חברתיות. הדוח מפנה אצבע מאשימה בעיקר למודיעין הצבאי הרוסי (GRU) ולשליחים ולמסייעים בידו כמו אתרי חדשות ואתרי הדלפות בראשם WikiLeaks. בפברואר וביולי 2018 הגיש התובע המיוחד וראש ה־FBI לשעבר רוברט מולר כתבי אישום מפורטים נגד כ־20 אזרחי רוסיה בגין התערבות במערכת הבחירות לנשיאות.[21] האישומים כוללים סעיפים רבים לרבות התחזות ופריצה למחשבי המפלגה הדמוקרטית (DNC). זהו כמובן אירוע ההתערבות בבחירות הבולט ביותר בשנים האחרונות, שתוצאתו ממשיכה להשפיע על ארצות הברית ועל העולם כולו.

ניתוח המעורבות הרוסית במבצעי השפעה על מערכות בחירות בעשור האחרון מעלה כי התקפות הסייבר בוצעו הן ישירות – באמצעות סוכנויות ממשל כגון המודיעין הצבאי הרוסי (GRU), שירות הביטחון הפדרלי הרוסי (FSB) או שירות ביון החוץ של רוסיה (SVR) שפעלו לשם גנבת מידע, הפצת מידע פוגעני, ייצור והפצה של מידע מטעה; פגיעה ושיבוש של שירותים; והן בעקיפין, באמצעות שימוש בשליחים (proxies) לא פורמליים כמו פושעי סייבר, חברות, יחידים וקבוצות של "האקטיביסטים" (hacktivists).[22] המטרות העיקריות של מעורבות רוסיה היו תמיכה במועמדים שרוסיה חפצה ביקרם והחלשת מועמדים שנתפסו כעוינים לקרמלין; החלשת המערכת הפוליטית המערבית ופגיעה בברית הטרנס־אטלנטית בין ארצות הברית למערב אירופה על ידי יצירת סכסוכים בין מדינות ובתוך המדינות שהיו יעד לתקיפה; וכן זריעת חוסר אמון ופגיעה במערכת הדמוקרטית בכללותה בין היתר על ידי טשטוש ההבחנה בין עובדות לבדיון.

מעדות מומחה שניתנה לפני ועדת המודיעין של הסנאט האמריקאי (יוני 2017)[23] ועסקה בהתערבות רוסיה בבחירות בגרמניה, עולה שמדובר בחלק ממערכה

21 The United States District Court for the District of Columbia, U.S.C. §§2, 371, 1030, 1028A, 1956 and 3551 et seq.) זמין בקישור: www.justice.gov/file/1080281/download

22 **שם**, בעמ' 9.

23 Stelzenmüller, *The Impact* **לעיל** ה"ש 13.

אסטרטגית נגד המערב בכללו, לרבות האיחוד האירופי, ארצות הברית והברית ביניהם. רוסיה התערבה במערכת הבחירות הגרמנית בשל חשיבותה הרבה של גרמניה באיחוד האירופי ובשל יחסיה המיוחדים עם רוסיה, עד שאלה התערערו לאחר פלישתה של רוסיה לחצי האי קרים. מאחר שבגרמניה אין משתמשים במכונות הצבעה, אלא בפתקי הצבעה בלבד והספירה אמנם ממוחשבת אבל נעשית במערכת סגורה ומוצפנת שאינה מחוברת לרשת האינטרנט – הסיכון העיקרי לגרמניה לא היה בהתערבות בביצוע הבחירות עצמן, אלא במניפולציות שכוונו לתודעת המצביעים.[24] על פי העדות, מערכת התעמולה שהופעלה בנוגע לבחירות בגרמניה התבססה על רשתות תקשורת רוסיות בשפה הגרמנית בשיתוף פעולה עם קבוצות מהימין הקיצוני ומהשמאל הקיצוני, נוסף על הגברה והדהוד של המסרים באמצעים טכנולוגיים כמו בוטים וטרולים.[25] בהקשר זה חשוב לציין כי יש מחקרים הטוענים שהשפעתם של המסרים המועברים ברשתות חברתיות על תודעת המצביעים אינה קבועה: בחברות שאינן מתאפיינות בשסעים חברתיים גדולים השפעתם אינה רבה;[26] ואילו במדינות שהחברה האזרחית בהן שסועה, יש בה תנועות פוליטיות קיצוניות רבות והשיח בה מפלג ואלים – פעילות זו להחלשת המשטרים הדמוקרטיים אפקטיבית במיוחד.

2. כיצד מבוצעות התקיפות?

המרחב המקוון מספק מגוון של אמצעים ושיטות להשפעה על מערכות בחירות בזירות שונות של תהליך הבחירות. מגוון זה נובע מהשינויים הדינמיים בסביבה

24 *Protecting German Political Party Sites* (BGProtect, March 19, 2018)

25 ראו להלן: "תקיפות של רשתות חבריות ואתרי חדשות".

26 Ulrike Klinger & Uta Russmann, *"Beer is More Efficient than Social Media" – Political Parties and Strategic Communication in Austrian and Swiss National Elections*, 14 Journal of Information Technology & Politics 299 (2017)

הטכנולוגית, מהיכולת להפיק מידע אישי רב, לנתחו ולהשתמש בו, מהשינויים באופן שהציבור צורך חדשות וממשקלן של הרשתות החברתיות. כלי ההשפעה שנעשה בהם שימוש הם בין היתר גנבת מידע מאישים פוליטיים והפצתו באופן ובמועד שיזיק ליריב; שיבוש מידע במערכת הבחירות – החל בשיבוש פנקס הבוחרים וכלה בשיבוש התוצאות – במטרה לערער את אמון הציבור בתוצאות הבחירות; מניעת שימוש במערכות מחשב החיוניות לניהול תהליך הבחירות באמצעות פגיעה במועד מתוכנן מראש; פגיעה במחשבי מערכת הבחירות גופא עד כדי שיבוש מהלכן; היכן שנהוגה הצבעה אלקטרונית – פגיעה במכשירי ההצבעה מבוססי המחשב; ייצור והפצה של חדשות כזב (fake news) ברשתות החברתיות; שיטוי בגורמים שלישיים באמצעות התחזות ברשת כמו למשל הונאת עיתונאים באמצעות הפצה של סרטוני וידאו ואודיו שמזויפים ברמה גבוהה מאוד כך שהתחקות אחרי האותנטיות שלהם קשה ביותר (deep fakes).[27] ניתן לשער כי השילוב בין היכולות המתעצמות של ייצור מידע מטעה לבין מנגנוני ההפצה המתוחכמים מבטיח כי השימוש באמצעים אלה רק יגבר.

להלן ייסקרו האמצעים העיקריים המשמשים להשפעה על תהליך הבחירות בהתאם לזירות ההשפעה השונות:

א. תקיפה של ביצוע הבחירות

ככלל ברוב המדינות תהליך ביצוע הבחירות מורכב משרשרת של אירועים ופעולות, שהעיקריים בהם הם: הכנה של ספר הבוחרים, הכולל רשימה מעודכנת של כל האנשים הרשאים על פי חוק להצביע בבחירות, ורק הם; הכנת רשימת קלפיות והקצאת רשימת הבוחרים הרשאית להצביע בכל קלפי; הודעה לבוחרים על הכללתם בספר הבוחרים ועל מיקום הקלפי שבה יוכלו לממש את זכותם להצביע; הפצת רשימות הבוחרים לקלפיות המקומיות; רישום המצביעים שהגיעו להצביע בפועל והשוואתה לרשימת הזכאים להצביע באותה קלפי; הצבעה – בנייר או במכונות הצבעה ממוחשבות; ספירת הקולות בכל

27 Robery Chesney & Danielle Citron, *Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?*, LAWFARE (February 21, 2018)

קלפי וקלפי; סיכום ספירת הקולות הכללי; חישובים שנגזרים מספירת הקולות (זהות המנצחים, מספר המנדטים).

כל החוליות הללו עלולות להיות יעדים פוטנציאליים לשיבוש, להיזק או לזיוף, ומכאן ההכרח להגן עליהן ביעילות. לדוגמה, קיומו של תהליך בחירות מחייב שימוש בכמה בסיסי נתונים שהחשוב שבהם הוא ספר הבוחרים – הקובץ שבו נכללים האנשים שעל פי החוק רשאי להצביע בבחירות. תקינותו של ספר הבוחרים – בין שמדובר בבחירות כלליות ובין שבבחירות מפלגתיות – קריטי בתהליך. כך למשל מחיקה של אחוזים ספורים מספר הבוחרים ערב הבחירות עלולה ליצור תוהו ובוהו ולמנוע את עצם האפשרות לקיים את הבחירות במועדן.[28] בסיס הנתונים הכללי הוא באחריות המדינה, אבל בסיסי נתונים רבים, בעיקר של מפלגות, אינם באחריותה, ומקימות ומתחזקות אותם חברות פרטיות, שאינן כפופות לרגולציה או לפיקוח מדינתי.

דוגמה לניסיון התערבות באמצעות תקיפה טכנולוגית ישירה של תהליך הבחירות עצמו התרחשה, כך לפי ידיעה שהודלפה בשנת 2017, לפני הבחירות לנשיאות בארצות הברית בשנת 2016, אז זוהתה פריצה מרחוק לחברה האמריקאית VR Systems, שמספקת ציוד ותוכנה לתהליך הבחירות.[29] על פי הידיעה, איתרה הסוכנות לביטחון לאומי (NSA) כי את הניסיון ביצעו האקרים רוסים שזוהו כקשורים למודיעין הצבאי הרוסי (GRU).

סיכון מיוחד קיים כשההצבעה נעשית במכונות הצבעה ממוחשבות, ולא בפתקי נייר, כמו למשל בכמה מדינות בארצות הברית. האיום הומחש בכנס Defcon בשנת 2017, אז הוצבה למשתתפי הכנס מכונת הצבעה כאתגר לפיצוח. למרבה המבוכה בתוך שעתיים הצליחו האקרים לשלוט בה שליטה מלאה.[30] בכנס הופגנו

28 Bruce Schneier, *American Elections are Too Easy to Hack. We Must Take Action Now*, The Guardian (April 18, 2018)

29 Matthew Cole, Richard Esposito, Sam Biddle, & Ryan Grim, *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, The Intercept (2017)

30 Matt Blaze, Jake Braun, Harri Hursti, Joseph Lorenzo Hall, Margaret MacAlpine, & Jeff Moss, *DEFCON 25 Voting Machine Hacking*

החולשות הרבות של מכונות ההצבעה, לרבות היכולת לשנות את התוצאות, להחדיר אליהן תוכנות זדוניות, ואף להרוס אותן הרס פיזי, מרחוק. יש לזכור כי מדובר בהאקרים שפרצו אל המכונות בזמן המוגבל של הכנס בלי שעמדו לרשותם משאבים מיוחדים. מכאן אפשר להניח בוודאות כי מדינה בעלת יכולות טכנולוגיות גבוהות ודי זמן להתכונן עשויה לבצע זאת ללא קושי מיוחד. יתר על כן, העובדה שמדובר בהצבעה שמטבעה חייבת להיות סודית, אינה מאפשרת להתחקות בדיעבד אחרי נכונות ההצבעה, ועניין זה מפחית עוד יותר את היכולת להבטיח את אמינותן של המכונות.[31]

תקיפת סייבר ישירה של ביצוע הבחירות עשויה להתבצע גם באמצעות פריצה למחשבים והשבתתם או גנבה מהם, וכן מניעת גישה לשירותים. דוגמה לכך הייתה בשנת 2015 בגרמניה, אז אלפי מחשבים שקשורים לבונדסטאג הודבקו בתוכנות זדוניות ודואר אלקטרוני נגנב משרתים של הבונדסטאג. בשל היקפה של ההתקפה הושבתו כל מחשבי הבונדסטאג לארבעה ימים. ההתקפה יוחסה לקבוצה ששמה APT28, הידועה גם בשמות Fancy Bear או Pawn Storm (שפרצה גם למחשבי המפלגה הדמוקרטית בארצות הברית, ראו להלן), וארגוני המודיעין המערביים מקשרים אותה אל המודיעין הצבאי הרוסי (GRU). מידע שנאסף מחשבונות הדוא"ל שנפרצו עלול לשמש תשתית לתקיפות עתידיות, גם כאלה שמטרתן להשפיע על תהליך הבחירות.

בישראל, קריסתו של האתר שהקים משרד הפנים כדי לעדכן את הציבור בתוצאות הבחירות לרשויות המקומיות[32] באוקטובר 2018, מלמדת על הפגיעות של המערכות הממוחשבות (במקרה זה מערכת פשוטה ביותר) הקשורות לשלבים שונים של ביצוע הבחירות, ועל הסכנה שפגיעה במחשבים אלה, שיבוש או מניעת שירות שהם נותנים תפגע באמון הציבור בתוצאות הבחירות.

Village (Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure, 2017)

31 Schneier, *American Elections*, **לעיל** ה"ש 28.

32 יסמין יבלונקו "בעקבות קריסת מערכת תוצאות הבחירות המקומיות: נשיא החברה שפיתחה אותה מתנצל" **גלובס** (4.11.2018).

ב. תקיפה של מפלגות ואישים פוליטיים

רבים מניסיונות הפגיעה בהליכי הבחירות בוצעו באמצעות פגיעה באתרים של מפלגות, אישים פוליטיים וארגונים תומכים, או השבתה שלהם.[33] דוגמה בולטת במיוחד היא הפריצה למחשבי המפלגה הדמוקרטית בארצות הברית בשנים 2015–2016 במטרה לפגוע בסיכוייה של המועמדת הילרי קלינטון. המודיעין האמריקאי וחברות אבטחה זיהו ששתי קבוצות האקרים הקשורות למודיעין הרוסי – שירות הביטחון הפדרלי (FSB) והמודיעין הצבאי (GRU) – פרצו למחשבי המפלגה, גנבו כמויות גדולות של מידע והפיצו אותו באופן מגמתי בזמן מערכת הבחירות.[34]

בעדותו לפני ועדת המודיעין של הסנאט ב־30 במרץ 2017 אמר פרופ׳ תומס ריד, מומחה לאבטחת מידע, כי בין 10 במרץ ל־7 באפריל 2016 סימנו שירותי ביון רוסיים עובדים במסע הבחירות של קלינטון, ושלחו להם 214 הודעות דואר אלקטרוני למטרת "פישינג" – השגת סיסמאות וגישה למחשב ולתוכן המצוי בו. בין היתר שלחו הודעות לכתובת הדוא"ל הישירה של קלינטון בניסיון מוצלח לגנוב סיסמה באמצעות קישור (לינק) לשינוי פרטי הסיסמה שלה. לאחר גנבתו הופץ המידע בשיטתיות, במועדים שנקבעו בכוונה, באמצעות אתר WikiLeaks.[35]

באפריל 2018 הגישה המפלגה הדמוקרטית תביעה אזרחית בניו יורק נגד רוסיה, שירות המודיעין הצבאי שלה (GRU), דונלד טראמפ, אתר ההדלפות WikiLeaks ושורה ארוכה של נתבעים. כתב התביעה מפרט את עילות התביעה שעיקרן – פריצה למחשבי המפלגה הדמוקרטית, גנבת עשרות אלפי מסמכים והפצתם לשם שיבוש קמפיין הבחירות של הילרי קלינטון בבחירות 2016. בכתב התביעה

33 Greenberg, *Everything We Know*, **לעיל** ה"ש 7.

34 Polyakova & Boyer, *The Future of Political Warfare*, **לעיל** ה"ש 19 בעמ' 10.

35 ראו דבריו של תומס ריד לפני הוועדה: Disinformation a Primer in Russian Active Measures and Influence Campaigns, Hearings before the Select Committee on Intelligence, United States Senate (March 30, 2017) (Thomas Rid, Opening Statement)

דורשת המפלגה הדמוקרטית, נוסף על פיצויים, גם הוצאת שורה של צווים נגד הנתבעים.[36]

מקרה נוסף של תקיפת מפלגה בארצות הברית אירעה, כך לפי החשד, בפריימריז של 2016, אז הותקף ספר הבוחרים של המפלגה הרפובליקאית, ומאות שמות של חברי המפלגה הרשאים להצביע בבחירות הפנימיות שונו.[37]

בצרפת נפרצו חשבונות דואר אלקטרוני של בכירים במסע הבחירות של מקרון, ותוכנם הופץ יומיים בלבד לפני הבחירות.[38] היעד העיקרי של התקיפות, המיוחסות אף הן לרוסיה, היה מפלגת En Marche בראשותו של עמנואל מקרון. כדי להיערך לאיום הרוסי, אסר מערך הסייבר הצרפתי (ANSSI) כליל על הצבעה ממוחשבת, וכן פנה לראשי המפלגות ומסר להם רשימה של חברות ומומחי אבטחת סייבר מאושרים כדי שיוכלו להיעזר בהם.[39] גם צוותי האבטחה של המפלגות – בעיקר של מקרון, שמפלגתו הייתה היעד העיקרי למתקפות – נקטו יוזמות כגון הצפת הרשת במידע כוזב במטרה ליצור "רעש תקשורתי" ובכך להפחית את האפקטיביות של גנבת מידע מהמפלגה. מקרון גם מינה (אנטי פייק ניוז קומנדו) של שלושה עורכי דין שפעלו בנחישות, במהירות וביעילות נגד הפצת המידע הכוזב ברשתות.[40]

ואולם למרות היערכות זו, חשבונות דוא"ל רבים של עוזרי מקרון נפרצו, ובאמצעות אתרי הדלפות כמו WikiLeaks הודעות דוא"ל הופצו יומיים בלבד

36 Matthew Kahn, *Document: DNC Sues Russia, Trump Campaign and WikiLeaks for Election Interference*, Lawfare (April 20, 2018)

37 Latanya Sweeney, Ji Su Yoo, & Jinyan Zang, *Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections*, Technology Science (2017)

38 Polyakova & Boyer, *The Future of Political Warfare*, **לעיל** ה"ש 19, בעמ' 6.

39 Erik Brattberg & Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, 26 (Carnegie Endowment for International Peace, 2018)

40 **שם**, בעמ' 27.

לפני הבחירות. חברת אבטחת המידע Trend Micro זיהתה את מקור ההדלפות באותה קבוצת האקרים שנזכרה למעלה – זו הידועה בשמות Pawn Storms, APT28 או Fancy Bear – קבוצה שהמודיעין האמריקאי קישר למודיעין הצבאי הרוסי (GRU).[41]

גם בגרמניה בשנת 2016 זיהה המודיעין הגרמני (BFV) פריצה למחשבי מפלגתה של אנגלה מרקל, פריצה שיוחסה לקבוצת האקרים בעלת קשר לממשלת רוסיה.[42]

תקיפות אלה מדגימות את הסיכונים הגלומים בהתקפות סייבר על מפלגות פוליטיות ועל שחקנים פוליטיים. ההתקפות עשויות להשפיע הן על הבחירות הפנימיות (הפריימריז) באופן שיטה את התוצאות לטובת מועמד מועדף או נגד מועמד שנתפס כפוגע באינטרסים של המעצמה המתערבת, והן על הבחירות הכלליות. יעדי הפגיעה עשויים להיות בין היתר רשימות התומכים/מתלבטים ודרכי הקשר עמם, אסטרטגיית הקמפיין עצמה, כספים ותורמים, ניהול מערך המתנדבים, ניהול מערך ההסעות ועוד עניינים רבים שעשויים להשפיע מאוד על ניהול הקמפיין הפוליטי, על יכולת ההתארגנות בפועל לבחירות, ובנוסף - להיות בסיס נוח למבצעי השפעה שתכליתם הטיית דעת הקהל.

ג. תקיפות של רשתות חברתיות ואתרי חדשות מקוונים

השימוש בכלי סייבר אינו מוגבל רק לתקיפות ישירות של מערכות מידע, אלא יכול לשמש, בעיקר באמצעות הרשתות החברתיות, להפצת מידע שקרי ולהטיית דעת הקהל למידע זה או אחר (גם כשמדובר במידע נכון). ההפצה נעשית למשל על ידי הדגשתו של מידע, הגברת תפוצתו וחשיפה נרחבת של הציבור אליו בין היתר בעזרת הפצת מידע ממוקד ש"נתפר" לפי ניתוח ההעדפות של בוחרים ספציפיים. זיהוי ה"פגיעות התודעתית"[43] של הבוחרים הוא הבסיס למבצעי השפעה מבוססי סייבר, שעשויים להיות יעילים לא פחות ממבצעים שמכוונים לפגוע במערכות המידע או להזיק להן. כך למשל בשנת 2018 חשפה חברת

41 **שם**, בעמ' 34.

42 Polyakova & Boyer, *The Future of Political Warfare*, **לעיל** ה"ש 19.

43 Stelzenmüller, *The Impact*, **לעיל** ה"ש 13, בעמ' 5.

Clearsky הישראלית מבצע השפעה איראני (בעשרות שפות) שמטרתו להשפיע על השיח הציבורי במדינות המערב לשם קידום האינטרסים של איראן.[44] התוקף עושה זאת כדי להחליש את המערכת הפוליטית ובכך את המדינה, ובין היתר הוא נשען על הקושי של ההנהגה הפוליטית לפעול נגד התקיפה משום שהיא עצמה מעורבת במערכת הבחירות ולכן כל פעולה מצידה חשודה מראש כמוטה לטובתה ולא לטובת המדינה.

מניפולציה על דעת הקהל באמצעות אתרי חדשות או רשתות חברתיות מתבצעת בדרך כלל בכלים טכנולוגיים, בכלי פריצה וגם במגיבים אנושיים:

• **בוטים – חשבונות פיקטיביים.** בוטים הם מחשבים שמריצים תוכנה מתוחכמת שמתחזה למשתמש אנושי לגיטימי[45] ומפרסמת רשומות (פוסטים) ברשתות החברתיות. בוטים אינם תופעת רשת שולית או זניחה,[46] שכן אפשר לשכפלם בהיקפים עצומים, וככל שהם מתוחכמים יותר, כך קשה יותר לזהות שמדובר בבוט. "צבא" של בוטים יכול להפיץ אינספור מסרים מעוררי מחלוקת, שנאה ואלימות ברשתות החברתית בצורה של רשומות או תגובות (טוקבקים) לכתבות בעיתונים המקוונים.

• **טכנולוגיות מבוססות נתוני עתק (Big Data).** השימוש בניתוח של נתוני עתק מאפשר לכוון את המאמצים לקהלים מסוימים, למשל לבעלי העדפות פוליטיות מסוימות או למשתמשים שעונים לפרופיל של "קלים להשפעה" בעקבות ניתוח התנהגותם ברשת ורשומות שהם העלו בעבר. כשהניתוח נעשה על נתוני עתק, למשל כל הנתונים ברשת פייסבוק, אפשר להגיע באופן ממוקד למשתמשים רבים.

• **כלי פריצה טכנולוגיים (האקינג).** תקיפה של אתרים וחשבונות אותנטיים ושיבוש המידע בהם. התוקף "משתלט" על חשבון לגיטימי, למשל על ידי גנבת הסיסמה, ומשתמש בו להפצת מידע כרצונו.

44 *Global Iranian Disinformation Operation*, Clearsky LTD (November 30, 2018)

45 Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, & Alessandro Flammini, *The Rise of Social Bots*, 59 (7) Communications of the ACM, 96 (2016)

46 Onur Varol, Emilio Ferrara, Clayton Davis, Filippo Menczer, & Alessandro Flammini, *Online Human-Bot Interactions: Detection, Estimation, and Characterization* (Arxiv ID: 1703.03107, 2017)

- **טרולים.** טרולים הם מגיבים מקצועיים בשכר (טוקבקיסטים בתשלום) שמתחזקים כמה זהויות פיקטיביות במקביל וכך יוצרים תגובות רבות.
- **התחזות לפורומים תמימים לגיוס עוקבים.** הקמת קבוצות ברשתות החברתיות בנושאים שבקונצנזוס (למשל "חיים בריאים") כדי להכין תשתית של עוקבים ל"יום פקודה".

מכתבי התביעה שהגיש התובע המיוחד וראש ה־FBI לשעבר רוברט מולר עולה כי בבחירות לנשיאות ארצות הברית ב־2016 התערבו גורמים רוסיים באופן נרחב בשיח הציבורי האמריקאי כדי לקדם את מועמדותו של דונלד טראמפ. סעיפי כתב האישום חושפים מתקפה מתוחכמת, שכוללת ארגונים וחברות שקיבלו מימון המוערך במיליוני דולרים במטרה להפיק מבצע השפעה רחב על השיח הפוליטי. מבצע ההשפעה השתמש ברשתות החברתיות כדי להפיץ מסרים שתומכים בטראמפ, ובמדינות כגון פלורידה ופנסילבניה כללו המסרים גם התחזות למוסלמים תומכי הילרי קלינטון ורכישת פרסומות בפייסבוק שבהן אמירות כגון "תמכו בהילרי. הצילו את המוסלמים האמריקאים" במטרה ליצור זיקה בינה ובין מוסלמים.

בפרסומים שונים נטען כי במשך שנים הפעילה רוסיה מערך של טוקבקיסטים אנושיים (טרולים), האקרים, בוטים ועוד במטרה להפיץ ולהעצים מסרים שיהדהדו במרחב השיח הציבורי במדינות דמוקרטיות. מסרים אלה נועדו לשרת את רוסיה על ידי יצירת פילוג ושסעים בחברה המערבית, תמיכה בתנועות ובמועמדים בעלי השקפות לאומניות קיצוניות, ערעור האמון של האזרחים במערכת הדמוקרטית ופגיעה בלכידות החברתית. החוקרים בסי ופררה ניטרו תוכן מהרשת החברתית טוויטר, ומניתוח ה"ציוצים" הם טוענים כי בתקופה שבין 16 בספטמבר ל־21 באוקטובר 2016 כ־400,000 מהחשבונות שהשתתפו בשיחות בנושא הבחירות לנשיאות ארצות הברית הופעלו כנראה באמצעות בוטים, כך שבוטים השתתפו בכ־19% מהשיחות בנושא בתקופה האמורה. אלה מספרים עצומים שממחישים את הנפח ואת האפקטיביות של שימוש יעיל בטכנולוגיה זו. הבוטים והטרולים יוצרים אפקט אדיר של הדהוד ברשת[47] ומגיעים לפלח נרחב מהציבור.

47 Lazer, Baum, Benkler, Berinsky, Greenhill, Menczer, Metzger, Nyhan, Pennycook, Rothschild, Schudson, Sloman, Sunstein, Thorson, Watts, & Zittrain, *The Science of Fake News*, 359 (6380) Science 1094 (2018)

לצורך קידום מבצעי ההשפעה ננקטו – בעזרת הכלים שהוזכרו למעלה – כמה שיטות פעולה עיקריות:

1. הפצת מידע מטעה (דיסאינפורמציה)

הפצת מידע מטעה כוללת ייצור מידע שקרי וכן הפצה של מסרים המעבירים תוכן כזה או תוכן מפלג ומעורר מחלוקת באופן שמגביר את החשיפה אליו. כיום הפלטפורמות המקוונות הן הזירות העיקריות המאפשרות הפצת מידע מסוג זה.[48] פעולות כאלה עשויות להתבצע בעזרת כלים גלויים כמו רשתות התקשורת השייכות לשלטון הרוסי או מופעלות על ידיו (RT (Russia Today), Sputnik או Ruptly TV) או בכלים חשאיים, בעיקר באמצעות טרולים ובוטים ברשתות חברתיות או הדלפות מכוונות לאתרים כמו WikiLeaks או DCLeaks.

מידע מטעה מכוון בדרך כלל לחזק נרטיבים פוגעניים, ולכן השימוש בכלי הסייבר – בין היתר באמצעות הפצה רשתית בממדים עצומים – נעשה במטרה לקבע את הנרטיבים הפוגעניים, לחזקם ולנטוע במספר גדול ככל האפשר של צרכנים את התחושה כי מדובר במידע מבוסס. כעולה מהניסיון של השנים האחרונות, הדרך המועדפת לכך היא זיהוי של נושאים מפלגים שנתונים במחלוקת ציבורית – כגון זהות לאומית ומיעוטים, יחס לאסלאם, מתחים גזעיים, טרור, יחס להגירה ולמהגרים, מתחים בין האיחוד האירופי למדינות הלאום – והעצמה שלהם.

במחקר שביצע מכון ראנד כונו שיטות פעולה אלה "הפצת מידע שקרי בעוצמה של צינור כיבוי" (Firehose of Falsehood),[49] כלומר הפצת מידע באופן מתמשך, חזרתי, במהירות רבה, בעוצמת הפצה גבוהה ובערוצים רבים. התוקפים גם אינם מחויבים לאמת העובדתית ואינם חשים חובה לפעול בעקביות. עקרון פעולה זה מבוסס על ההבנה כי לרושם הראשוני משקל רב בעיצוב התודעה, וכי לאחר היחשפות חוזרת מסר נוטה להיקלט (כמו שאכן עולה ממחקרים שהראו כי חזרתיות מביאה לידי היכרות פמיליארית ומכאן לקבלת המסר).[50] המטרה של

48 שם.

49 Christopher Paul & Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (Policy file) (RAND Corporation, 2016)

50 שם.

הפצת מידע כזה איננה מכוונת רק להשפיע לכיוון מועמד זה או אחר, אלא גם לטשטש את ההבדל בין עובדה לבדיון, לערער את אמון הציבור באמינות של דיווחים תקשורתיים בכלל, ועל ידי כך - את אמון הציבור בשיטה הפוליטית כולה.

דוגמה להפצת דיסאינפורמציה הייתה פרשת "ליסה" בשנת 2016 בגרמניה – נערה ממוצא גרמני־רוסי שנטען כי מהגר ממוצא ערבי בגרמניה תקף אותה מינית. הסיפור הומצא, הופץ ומוחזר ברשתות התקשורת הרוסיות במטרה לעורר רגשות נגד מהגרים ונגד מדיניות ההגירה של קנצלרית גרמניה אנגלה מרקל, ובעקבותיו התקיימו הפגנות רבות נגד מרקל.[51]

בבחירות לנשיאות צרפת באפריל־מאי 2017 זוהה שהמודיעין הרוסי משתמש בפייסבוק כדי להפיץ מידע מטעה נגד מקרון.[52] גם בבריטניה נמשכות החקירות בנוגע לחשד כי רוסיה עמדה מאחורי מבצעי השפעה ברשתות החברתיות בזמן הברקזיט[53] באמצעות בוטים[54] שהפיצו מסרים נרחבים התומכים בפרישת[55] בריטניה מהאיחוד.

51 Stefan Meister, *The "Lisa Case": Germany as a Target of Russian Disinformation*, NATO Review (2016)

52 Polyakova & Boyer, *The Future of Political Warfare*, **לעיל** ה"ש 19.

53 ראו אצל Brattberg & Maurer, *Russian Election Interference*, **לעיל** ה"ש 39, בפסקה 84:

> The Digital, Culture, Media and Sport Committee in the House of Commons launched an investigation in September 2017 into Russia's use of social media during the [Brexit] referendum campaign.

54 Yuriy Gorodnichenko, Tho Pham, & Oleksandr Talavera, *Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #USElection* (NBER Working Papers 24631) (National Bureau of Economic Research, 2018)

55 Matthew Field & Mike Wright, *Russian Trolls Sent Thousands of Pro-Leave Messages on Day of Brexit Referendum, Twitter Data Reveals*, The Telegraph (17.10.2018)

2. איסוף מידע אישי ושימוש בו להשפעה

השגת מידע אישי רב ערך על משתמשים ללא ידיעתם והשימוש בו באמצעות כלים רבי עוצמה מהתחום של ניתוח נתוני עתק (Big Data) אינו חדש, אבל ההיקף והעוצמה של היכולות הגלומות בטכנולוגיה זו מתגברים בקצב מסחרר.

כבר בשנת 2014 פרסמה רשות הסחר של ארצות הברית (FTC) דוח ובו קבעה כי חברות אספו עד 3,000 פרטי מידע אישי על כל אחד מהמשתמשים בשירותיהם ללא ידיעתם.[56] אחת החברות העיקריות (Acxiom Corporation) החזיקה מידע על כ־200 מיליון אמריקאים.[57]

בתחום הפוליטי הדוגמה הבולטת ביותר היא פרשת *Cambridge Analytica*, שפורסמה בתחילת 2018. מהפרסומים עולה כי החברה אספה מתוך הרשת החברתית פייסבוק מידע על כ־240 מיליון אמריקאים[58] (ועוד מאות מיליונים בעולם כולו), בין היתר לשם הפצה אוטומטית של תעמולה ממוקדת ומותאמת בהתאם לניתוח הפרופיל של המשתמשים (מיקרו־טרגטינג).[59] החברה ניצלה פרצה בפייסבוק שאפשרה לה לאסוף נתונים דמוגרפיים ואחרים גם על משתמשים שלא הסכימו לכך, ועל ידי כך הפרה את חוקי הפרטיות. כך צברה החברה נכס חשוב של נתונים על המשתמשים. מידע זה שימש את החברה לצורך בנייה אוטומטית של פרופילים של סוגי משתמשים והפצה אליהם של מידע ממוקד המותאם לפרופיל שהוכן עבורם, באופן שיכול היה להשפיע בסבירות גבוהה יותר על העדפותיהם הפוליטיות. כך קמפיינים ברשתות החברתיות נעשו אפקטיביים יותר למי שהתכוון להשפיע על מערכת הבחירות.

56 Federal trade commission, *Data Brokers: A Call for Transparency and Accountability* (A Report of the Federal Trade Commission) 47 (May 2014)

57 Polyakova & Boyer, *The Future of Political Warfare*, **לעיל** ה"ש 19, בעמ' 11.

58 Carole Cadwalladr, *British Courts May Unlock Secrets of How Trump Campaign Profiled Us Voters*, Sun (October 1, 2017)

59 Patrick Greenfield, *The Cambridge Analytica Files: The Story So Far*, The Guardian (March 26, 2018)

3. הפצה והגברה של מידע נכון אבל מוטה

אחד הכלים היעילים ביותר להשפעה על התודעה הוא שימוש מוטה במידע שהושג באמצעות פריצה בכלי סייבר, הפצתו, הגברתו ויצירת השפעה חברתית באמצעות הרשתות החברתיות. בשיטה זו משתמשים לעיתים במידע שנגנב מהתכתבות אישית ופרטית בין חברים, שעלולה לכלול התבטאויות בעייתיות, מידע אישי מביך וכדומה. הפצה מוגברת של המידע באמצעות בוטים וחשבונות פיקטיביים עשויה להביאו לידיעתם של המוני אנשים, ומכאן גם לזליגתו לכלי תקשורת ממוסדים. דוגמה לכך הייתה הודעות הדוא"ל שנגנבו בקמפיין של עמנואל מקרון: ההודעות שנגנבו הופצו יומיים לפני מועד הבחירות, באמצע מאי 2017, והוגברו ברשתות כך שבתוך שעות ספורות נמנו כ־50,000 ציוצים בטוויטר, רובם מחשבונות פיקטיביים.[60] לפני בחירות אלה הועלו כ־9 ג'יגה בייט של מידע ו־21,000 הודעות שנגנבו ממטהו של מקרון לאתר *Pastebin* תחת שם המשתמש EMLEAKS, ולאחר מכן הועלו שוב באתר *WikiLeaks*. נוסף על החומרים הגנובים הופצו על מקרון – באמצעות בוטים שמזוהים עם אתרים פרו־רוסיים – שמועות, בין היתר שהוא סוכן אמריקאי, שהוא הומוסקסואל מוסתר ושהסעודים ממנים אותו.[61]

4. תקיפות סייבר נגד תשתיות קריטיות

על בחירות אפשר להשפיע גם באמצעות פגיעה בתשתיות חיוניות הן במטרה לעורר זעם אזרחי, והן כדי לשבש את תהליך הבחירות עצמו. כך למשל באוקראינה כללה המתקפה הרוסית גם התקפה מתוכננת היטב על מערכת החשמל, שבדצמבר 2015, יום לפני חג המולד, הביאה לידי השבתה של אספקת החשמל – כולל השבתה של גנרטורי החירום – לכ־230,000 תושבים.[62]

60 Polyakova & Boyer, *The Future of Political Warfare*, **לעיל** ה"ש 19, בעמ' 6.

61 Brattberg & Maurer, *Russian Election Interference*, **לעיל** ה"ש 39.

62 Polyakova & Boyer, *The Future of Political Warfare* **לעיל** ה"ש 19, בעמ' 13.

תשתיות קריטיות אפשר לתקוף – ממניעים פוליטיים או כדי להשפיע על המערכת הפוליטית – גם באמצעות הדבקה בווירוסים, ואלה עשויים להתפשט גם למדינות אחרות. כך למשל בשנת 2018 הזיק הווירוס NotPetya לחברות ולארגונים ממשלתיים ב־64 מדינות. הודעה רשמית מטעם ממשלת ארצות הברית (פברואר 2018) ייחסה את הפצת הווירוס לצבא הרוסי.[63] בדומה ייחסו שירותי הביון הבריטים והאמריקאים את הפצתו של הווירוס Wannacry, שפגע בבתי חולים במערב, לצפון קוריאה.[64]

עם זה בשנים האחרונות ניכרת מגמה לעבור מהתקפות סייבר קלסיות – שמכוונות נגד תשתיות ומניעת שירותים חיוניים – להתקפות "רכות", שמשלבות ריגול סייבר וגנבות באמצעות כלי סייבר יחד עם מניפולציה ופרסום מוטה, סלקטיבי ומכוון כמו שפורט בסעיפים הקודמים.[65]

3. דרכי ההתגוננות העיקריות שנקטו מדינות אחרות

מהתקפות הסייבר על מערכות הבחירות בארצות הברית ובמדינות המערב בשנים האחרונות עולה כי אף מדינה אינה יכולה להרשות לעצמה להישאר שוות נפש לנוכח האיום. נדרשת שורה של פעולות הן במישור ההגנה והן

63 Statement from the Press Secretary in June 2017, The Russian Military Launched the Most Destructive and Costly Cyber-Attack in History (The White House, February 2018)

64 The Foreign Office Minister & Lord Ahmad of Wimbledon, *Foreign Office Minister condemns North Korean actor for WannaCry attacks* (GOV.UK, December 19, 2017)

65 Jack Goldsmith & Stuart Russell, *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations* (Hoover Aegis Series Paper No. 1806) (Hoover Working Group on National Security, Technology and Law, June 5, 2018)

במישור ההרתעה כדי לחזק במידה ניכרת את כושרן של הדמוקרטיות להתגונן ביעילות נגד התקפות כאלה.[66] ואולם כשדמוקרטיה ליברלית מבקשת להתגונן מפני התקפות שמאיימות על עצם יכולתה לקיים את תהליך הבחירות ואף מביאות לידי ערעור אמונו של הציבור בתהליך זה, עולות שאלות עקרוניות רבות שעיקרן: מהם הגבולות בין שימוש לגיטימי בכלי השפעה בין מדינות, למשל "עוצמה רכה",[67] ובין פעולת חתרנות זדונית; וכיצד להבטיח כי פעולות התגוננות מפני ההתקפות המכוונות לא יפגעו בעצמן בעקרונות הדמוקרטיה הליברלית כגון שמירה על חופש הביטוי, שמירת הפרטיות ושוויון. במילים אחרות אסור שחיזוק האמצעים להגנת הדמוקרטיה יביאו לידי הגבלת השיח הפוליטי ולהגברת הפיקוח על האזרחים, בבחינת שפיכת התינוק עם מי האמבט.

יישום עקרונות אלה מעלה שאלות בנוגע לגבולות הפעולה כגון: האם לדמוקרטיה מותר להתגונן מפני התערבות של מדינה זרה באמצעות תעמולה נגדית (שקרית) או באמצעות תקיפות־נגד (Hack back)? מתי התגוננות יעילה חוצה את הקו של צנזורה פוליטית? או מהי מדיניות הפיקוח הרצויה של הממשלה והפרלמנט על פעולותיהם של ארגוני הביטחון והמודיעין בנושא? שאלות נוספות עולות בנוגע ל"גביית מחיר" מהיריב במישור הטכנולוגי ואף במישורים אחרים. רעיונות אלה, בעיקר בכל הנוגע לתגובה נגד משטרים סמכותניים, כלולים במונח "עוצמה חדה" (Sharp Power) שנטבע בשנת 2017[68] ועיקרו – נקיטת צעדים אגרסיביים יותר נגד מדינות אוטוריטריות, בעיקר רוסיה וסין, בלי לפגוע בערכים הדמוקרטיים.[69] יש לזכור כי הנרטיב הרוסי גורס

66 Brattberg & Maurer, *Russian Election Interference*, **לעיל** ה"ש 39.

67 Joseph Nye, Bound to Lead: The Changing Nature of American Power (1990)

68 Christopher Walker & Jessica Ludwig, *The Meaning of Sharp Power*, Foreign Affairs (November 16, 2017)

69 Joseph Nye, *How Sharp Power Threatens Soft Power: The Right and Wrong Ways to Respond to Authoritarian Influence*, Foreign Affairs (January 24, 2018)

כי רוסיה מתגוננת מפני המערב בשיטות ובאמצעים שמופעלים נגדה,[70] ומכל מקום, עד כה הכחישה רוסיה את ההאשמות[71] וטענה כי בשום מקרה לא הופר החוק הרוסי.[72]

בשנים האחרונות, במטרה להתגונן מפני התקפות סייבר על תשתיות לאומיות ובכלל זה להגן על תהליך הבחירות, הקימו מדינות רבות מרכזים להגנת סייבר ויחידות לתגובה מהירה (CERT), נקטו פעולות רבות להגנת הרשת הממשלתית, ובמסגרת צבאית הקימו גם "פיקוד סייבר" במתכונת זו או אחרת. עוד אותר הצורך בשיתוף פעולה והעברת מידע בין מדינות, בראש ובראשונה לשם שיפור יכולת הייחוס (attribution) של ההתקפה כך שניתן יהיה לשכנע, בראש ובראשונה מבחינה ציבורית, מי עומד מאחורי התקיפה.[73] עוד נוסחו אמנות חברתיות, למשל כאלה המחייבות ייחוס של כל מודעה או מסר פוליטי במערכת בחירות.

ממכלול הצעדים שנקטו מדינות אחרות או הוצעו על ידי חוקרים ומכוני מחקר במקומות אחרים בעקבות הניסיון המצטבר, עולה כי יש צורך בשורה ארוכה של צעדים כדי לשפר את ההגנה על מערכת הבחירות, במובנה הרחב, מפני התקפות סייבר – לרבות שיפור בתפיסת האיום, בדרכי הסיכול, התגובה וההרתעה; וכן פיתוח כלים מתאימים לניטור, לייחוס ולזיהוי התקיפה והתוקף.

מבחינה מעשית אפשר לחלק את דרכי ההתגוננות בהתאם ליעדי התקיפה, כדלקמן:

70 ראו למשל האשמות כלפי גוגל ויו־טיוב בהתערבות בבחירות ברוסיה: *Google Accused by Moscow of Meddling In Russian Elections*, Washington Times (September 4, 2018)

71 ריאיון של שר החוץ הרוסי, לברוב בפברואר 2018: *Russian Foreign Minister Sergei Lavrov Responds Charges in Meddling Probe*, CBS News (February 16, 2018)

72 ריאיון שנתן הנשיא הרוסי פוטין לרשת NBC (מרץ 2018): *Exclusive: Putin Addresses 2016 Election Meddling*, NBC News (March 3, 2018)

73 Stelzenmüller, *The Impact* **לעיל** ה"ש 13, בעמ' 5.

א. התגוננות מפני תקיפה ישירה על ביצוע הבחירות

א. הכרזה משפטית על הבחירות כ"תשתית קריטית"

במדינות רבות ההכרזה על מערכת כתשתית קריטית גוררת אחריה שורה של הוראות רגולטוריות ומקדמת הגדרת אחריות וקביעת תקנים לאבטחה. כך, בינואר 2017 הכריזה המחלקה לביטחון המולדת של ארצות הברית (Homeland Security) על הבחירות כתשתית קריטית[74] ומייד לאחר מכן, במרץ 2017, הקציב הקונגרס 380 מיליון דולר לשדרוג מערכות הבחירות.

ב. שדרוג מערכת המחשוב של הבחירות

ההבנה שקשה להבטיח חסינות מפני התקפות סייבר מביאה לידי המסקנה שעל המערכת הממוחשבת של ביצוע הבחירות לאפשר שחזור של הנתונים, ולשם כך יש לוודא כי מתבצעים גיבויים ברמה הנדרשת. על הגיבויים להיעשות במגוון אמצעים לאורך כל תהליך הבחירות – החל בספר הבוחרים, עבור במערכת המחשוב של ספירת הקולות וכלה בחישוב התוצאות. כך למשל נשמרים באופן מאובטח פתקי ההצבעה המקוריים של כל קלפי וקלפי כך שבמידת הצורך ניתן יהיה לחזור ולספור את הקולות.

ג. שימוש בפתקי הצבעה ולא במכונות הצבעה

לדעת מומחי אבטחה בכירים,[75] כיום אי־אפשר ליצור מערכת הצבעה ממוחשבת שתהיה מאובטחת דיה כך שמעצמה זרה לא תוכל בשום פנים ואופן לפרוץ אליה, לכן חייבים להמשיך ולבחור בפתקי הצבעה. גם אם אפשר לסרוק את פתקי ההצבעה – כדי לאפשר ספירה ממוחשבת – דרישת הגיבוי מחייבת שהנייר המקורי שעליו סומנה ההצבעה יישמר למטרות שיחזור. כך למשל בשנת 2009 אסר בית המשפט בגרמניה על הצבעה במכונות הצבעה ממוחשבות מהטעם

74 Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, U.S Homeland Security (January 6, 2017)

75 Schneier, *American Elections*, **לעיל** ה"ש 28.

ששימוש במכונות כאלה מנוגע לעקרונות האמינות והשקיפות של ההצבעה.[76] גם בהולנד, לקראת בחירות 2017, החליטה הממשלה לדבוק בשיטת הבחירות בנייר ולא לעבור להצבעה אלקטרונית.[77]

ד. תיעוד שינויים ושמירתם

כאשר נעשה שימוש במערכת ממוחשבת בתהליך הבחירות, מערכת זאת צריכה להיות מסוגלת לזהות ולתעד כל שינוי (Audit), תוספת או מחיקה שבוצעו בה. את השינויים יש לשמור בנפרד במדיה של "רישום בלבד" (write-only media) או להדפיסם על נייר.[78]

ה. הקמת כוח משימה ייעודי

בינואר 2018 הודיעה ממשלת בריטניה על הקמת כוח משימה ייעודי (National Security Communications Unit) שמשימתו להילחם במידע מטעה שאת הפצתו מכוונים שחקנים מדינתיים או אחרים. יחידה זו מדווחת ישירות לקבינט.[79]

ב. התגוננות מפני תקיפות נגד מפלגות ואישים פוליטיים

א. הבנה שמפלגות ואישים פוליטיים הם יעדים עיקריים לתקיפה

מההבנה כי מפלגות ואישים פוליטיים – לרבות עוזרים פוליטיים וחברות פרטיות שקשורות לניהול הפעילות הפוליטית – הם שחקנים עיקריים שעלולים להיות יעדים לתקיפה ועל כן יש לראות בהם יעדים להגנה, נגזרו גם המשמעויות המעשיות הנדרשות. כך למשל במערכת הבחירות במאי־יוני 2017 בצרפת ננקטו פעולות נגד ההתערבות הרוסית שכוונה בעיקר נגד מפלגתו של עמנואל מקרון, *En Marche*. לא הייתה זו יד המקרה: בעקבות תקיפת הסייבר נגד המפלגה

76 Brattberg & Maurer, *Russian Election Interference*, **לעיל** ה"ש 39, בפסקה 108.

77 Sewell Chan, *Fearful of Hacking, Dutch Will Count Ballots by Hand*, The New York Times (1.2.2017)

78 Schneier, *American Elections*, **לעיל** ה"ש 28.

79 Brattberg & Maurer, *Russian Election Interference*, **לעיל** ה"ש 39, בפסקה 82.

הדמוקרטית בארצות הברית ב־2016 שלח מזכיר ההגנה בלשכת נשיא צרפת מכתב לראשי המפלגות ובו הזהיר מפני תקיפות סייבר, ומערך הסייבר הלאומי הצרפתי (ANSSI) העביר לראשי המפלגות מסמכים מפורטים ובהם המלצות איך להתגונן מפני מידע מטעה ומפני תקיפה שמכוונת למניעת שירות (DDoS). משנחשפו ההתקפות, הודות לשילוב בין חקיקה ואזהרות של ועדת הבחירות המרכזית בצרפת, המסמכים שנגנבו ממטה מקרון לא זכו בסופו של דבר לתפוצה נרחבת, ורוב הצרפתים לא נחשפו אליהם.[80]

ב. גיבוש תפיסה כוללת

במדינות אחדות הובן כי צריך לגבש תפיסה כוללת לניטור, לפיקוח ולאסדרה של אבטחת מפלגות ואישים פוליטיים מפני תקיפות סייבר, שתיקח בחשבון את הבעייתיות הגלומה בהתערבות מדינתית בתאגידים מיוחדים כמו מפלגות פוליטיות; עוד גובשה ההבנה כי יש לקבוע תהליך מוסדי מובנה, בעל מקור מימון ברור, לשיפור יכולת ההגנה של מוסדות ומפלגות פוליטיות.[81]

ג. התגוננות מפני תקיפות על תודעת הבוחרים

א. עידוד הקמתה של מערכת רחבה לניטור ולבדיקת עובדות

במדינות אחדות התגבשה ההכרה כי יש מקום להקים גופים כגון מכוני מחקר ואפילו אתרים פרטיים שיפעלו כדי לבדוק, לחשוף ולהבהיר לציבור מהו מידע שקרי, מניפולטיבי ומכוון. מוסדות כאלה הם למשל ה־StopFake האוקראיני, או ה־EEAS (European External Action Service) של האיחוד האירופי – כמשאב מרכזי ל"חיסון" תודעת הציבור נגד הטיה מכוונת.

ב. פעולות של בדיקת עובדות

לאחר בחירות 2017 יזמה השרה ההולנדית אולונגרן (Kasja Ollongren) בשיתוף פעולה עם פייסבוק, עם אתר חדשות הולנדי ועם אוניברסיטת ליידן את הקמתו של אתר "בדיקת עובדות" (fact check) שמתפרסמות ברשתות החברתיות.[82]

80 **שם**, בעמ' 56.

81 Stelzenmüller, *The Impact*, **לעיל** ה"ש 13.

82 Brattberg & Maurer, *Russian Election Interference*, **לעיל** ה"ש 39.

ג. הסכמים בין מפלגות פוליטיות

בגרמניה למשל הסכימו ביניהן המפלגות הפוליטיות שלא להשתמש בבוטים זו נגד זו;[83] הרציונל הוא כי קיומו של הסכם מעין זה עשוי לסייע לחשיפת התערבות חיצונית, אם זו משתמשת בבוטים, במערכת הבחירות.

ד. שיתוף בין מדינות לענקיות התקשורת

משקלן הגובר של ענקיות התקשורת ויחסיהן עם המדינות הם נושאים מורכבים. השימוש ברשתות החברתיות כבסיס למבצעי השפעה הוליד חשיבה על הצורך לייסד מנגנוני שיתוף מידע, וולונטריים או רגולטוריים, בין מדינות מערביות ובין ענקיות התקשורת – פייסבוק, טוויטר וגוגל במטרה לייסד מערכת התראות ומוניטורינג. יש לציין כי עניין זה מעורר התנגדות רבה, בעיקר באירופה,[84] בין היתר משום שענקיות התקשורת אינן יכולות או צריכות לשמש "קבלן צנזורה" של מדינות, והענקת סמכויות לחברות אלה תוביל בהכרח לצנזור יתר ולפגיעה בחופש הביטוי. טענה זו תקפה גם כשמדובר בחקיקה מחייבת ולא רק בשיתוף פעולה וולונטרי.[85]

ה. כלי ניטור

השימוש בבוטים העלה, הן בקרב ענקיות התקשורת והן בהצעות מומחים,[86] את ההכרח בפיתוח כלי זיהוי וניטור מתקדמים למניעת חשבונות מזויפים/אוטומטיים.

83 Stelzenmüller, *The Impact*, **לעיל** ה"ש 13.

84 **שם**, בעמ' 11.

85 ראו למשל את הביקורת נגד החקיקה הגרמנית המחייבת את ענקיות התקשורת להסיר פרסומים לא חוקיים, לרבות הסתה לגזענות, הסתה לטרור ועוד בחוק המכונה NetzDG (Act to Improve Enforcement of the Law in Social Networks; ובמקור – Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken); Diana Lee, *Germany's NetzDG and the Threat to Online Free Speech,* MFIA (October 10, 2017)

86 Lazer et al., *The Science of Fake News,* 359 (6380) SCIENCE 1094 (2018)

ו. יכולות ייחוס

בעקבות הצורך להבין מי עומד מאחורי מבצע ההשפעה, להצביע עליו ולסמן אותו, הציעו מומחים מגוון של הצעות87 לפיתוח יכולות ייחוס יעילות, שקופות ומשכנעות; כלומר פיתוח יכולות טכנולוגיות מתקדמות שמאפשרות לסמן את הגורם המתערב. בשל אופייה של הרשת מדובר באתגר טכנולוגי מורכב. עוד ידרוש הדבר שיתוף פעולה בין מדינות, משום שבדרך כלל "המייל האחרון" בייחוס מצריך גישה לספקי האינטרנט המקומיים. יכולות אלה צריכות לאפשר שקיפות בכל הנוגע לאופן מנגנון הייחוס פועל.

ז. מניעת שימוש במידע אישי לשם מיקרו־טרגטינג פוליטי

בעקבות פרשת קיימבריג' אנליטיקה הוצע – למשל בארצות הברית – לקבוע נורמה ולצידה לייסד מנגנוני הענשה של חברות פרסום שיימצא שהפרו נורמה זו והשתמשו במיקרו־טרגטינג פוליטי; עוד הוצע לחייב חברות שאוגרות מידע, לתת למשתמשים גישה למידע שנאגר עליהם ואפשרות למחוק אותו אם רצונם בכך.[88]

ח. העלאת מודעות ציבורית

חוקרים הצביעו על החשיבות שבהעלאת ההבנה הציבורית בדבר האפשרות למניפולציה, בעיקר ברשתות חברתיות, כחלק חשוב מההתגוננות מפניה. העלאת המודעות מצריכה שילוב של פעולות ממשלתיות, פעולות של ענקיות התקשורת – לרבות פיתוח טכנולוגיות מתאימות לזיהוי ולניטור של מקורות להפצת מידע מטעה – וכן עידוד עמותות מהמגזר השלישי לחשוף ולפרסם שימוש במידע מטעה והפצה שלו.[89]

87 Stelzenmüller, *The Impact*, **לעיל** ה"ש 13.

88 Jim Isaak & Mina J. Hanna, *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*, 51 (8) Computer 55–56 (August 2018)

89 Darrell M. West, *How to Combat Fake News and Disinformation*, Brookings (December 18, 2017)

ט. הצבעה ישירה של אישים בכירים על הגורמים הפועלים להטיית הבחירות בשירות מעצמה זרה.

בהקשר זה התבטא בפומבי עמנואל מקרון עצמו ואמר כי אסר על עיתונאים משני כלי תקשורת המזוהים עם הקרמלין (RT ו־Sputnik) להיכנס לאירועי בחירות של מפלגתו משום שהם משמשים כ"סוכני השפעה" של רוסיה.[90] נעיר כי האשמות שאינן מבוססות דיין הן חמורות כשלעצמן.

4. תקיפות סייבר במדינות המערב במטרה להשפיע על הליך הבחירות - סיכום

מניתוח של תקיפות הסייבר על מערכות בחירות שבמדינות בעולם בשנים האחרונות, נראה כי הגורמים העיקריים העלולים לסכן באופן ממשי את תהליך הבחירות – על היבטיו – הם בעיקר ישויות בעלות יכולות מדינתיות, גם אם בפועל חלק מהפעולות נעשות באמצעות ארגונים או יחידים. אף שיש חוקרים שמטילים ספק בהשפעתן הממשית של תקיפות הסייבר – כך למשל יש הטוענים שהמגמות החברתיות והפוליטיות בחברה האמריקאית היו תוצאה של זרמי עומק, והמניפולציות שנעשו כדי להגבירן השיגו, בסופו של דבר, תוצאה שולית בלבד[91] – הפוטנציאל הקיים בתקיפות אלה לפגיעה בדמוקרטיה – אם בדרך של השפעה לכיוון בחירתו של מועמד ואם בדרך ערעור הציבור בתקינות ההליך הדמוקרטי – אינו מוטל עוד בספק. גם אם בסופו של דבר היקף הפגיעה בפועל אינו רב, התערבויות מסוג זה עלולות להשפיע על ליבת ההליך הדמוקרטי,

90 ראו Brattberg & Maurer, Russian Election Interference, **לעיל** ה"ש 39: Russia Today [RT] and Sputnik were agents of influence and propaganda that spread falsehoods about me and my campaign.

91 Yochai Benkler, Robert Faris, & Hal Roberts, Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics, 385 (2018); *Compendium on Cyber Security of Election Technology* (CG Publication 03/2018) (UN – NIS Cooperation Group, 2018)

שבבסיסו ערכים כמו חופש הבחירה, הוגנות ההליך וסודיות הבחירה האישית; ובעיקר באמון הציבור בכך שתוצאות הבחירות משקפות את הצבעת הבוחרים.

הניסיון המצטבר מלמד על שלושה אזורי תקיפה עיקריים: הליך ביצוע הבחירות על כל שלביו – אם בזיוף ואם בשיבוש ובמניעת שירות; מפלגות פוליטיות ושחקנים פוליטיים – גנבת חומר אישי ופוליטי ופרסומו בעיתוי מתאים, שיבוש היערכות המפלגה לבחירות ועוד; והרשתות החברתיות ואתרי החדשות – המאפשרים השפעה על תודעת הבוחרים. הדרכים העיקריות לתקיפה מבוססת סייבר על תהליך הבחירות כוללת שימוש בכלים טכנולוגיים כמו בוטים וטכנולוגיות מבוססות נתוני עתק (Big Data); שימוש בכלי פריצה טכנולוגיים על ידי מומחי פריצה (האקינג); שימוש במגיבים מקצועיים (טרולים) ובפלטפורמות התחזות כמו פורומים "תמימים" ועוד. כלים אלה שימשו להשפעה על בחירות למשל באמצעות מבצעי השפעה להפצת מידע מטעה והבאתו לקהל גדול מאוד; גנבת מידע והפצתו הסלקטיבית במועד המתאים להשפעה מרבית על הבחירות; מבצעי השפעה מכוונים אישית (מיקרו־טרגטינג); או השפעה דרך פגיעה בתשתיות. המשותף למהלכי השפעה אלה הוא המאמץ להסתיר את מקור התקיפה, ומכאן הקושי לאתר במועד מי הגורם העומד מאחוריה, וליחסה לתוקף ברור ומזוהה.

כמפורט בפרק זה, מדינות שונות נקטו פעולות שנועדו לסכל או למנוע את ההשפעה על מערכות בחירות. פעולות אלה מתבטאות בצעדים מוסדיים ורגולטוריים כמו הכרזה על תהליך הבחירות כתשתית קריטית – על המשתמע מכך מבחינת ההשקעה המדינתית בהגנה ובאבטחה לרבות מפני תקיפות סייבר; בצעדים שנועדו להגביר את מודעות הציבור; או בפיתוח יכולות לניטור תקיפה ואיתור המקור לה.

פרק ב
ניתוח תהליך הבחירות בישראל בהתאם לשלוש זירות התקיפה העיקריות

ישראל היא חברה משוסעת ומקוטבת, ובסוגיות כמו יחסי יהודים־ערבים, דת ומדינה, עתיד השטחים ועוד יש בה מתחים פנימיים עמוקים. לפיכך לפגיעה בהסכמה החברתית בנוגע למנגנון הבחירות כמופע הדמוקרטי העיקרי וכמקור ללגיטימציה השלטונית, ולכרסום באמון הציבור בתוצאות הבחירות עלולה להיות השפעה הרסנית במיוחד על החישוקים החברתיים המאפשרים את ניהול המחלוקות בחברה. מכאן חשיבותה המיוחדת של ההגנה על תהליך הבחירות במובנו הרחב.

בדומה לדמוקרטיות אחרות, גם בישראל תהליך הבחירות מורכב מכמה תהליכי משנה וזירות פעולה: ביצוע הבחירות לכנסת; המפלגות והשחקנים הפוליטיים; והרשתות החברתיות ואתרי החדשות המקוונים. תקיפת סייבר של אחת הזירות האלה או כמה מהן עלולה לפגוע בתהליך הבחירות ובאמון הציבור בתוצאותיו.

.1
ביצוע הבחירות: התהליך ואפשרויות הפגיעה

כדי לבחון מהם האזורים הפוטנציאליים העיקריים בביצוע הבחירות שעליהם יש להגן מפני תקיפה מבוססת סייבר, נתאר את השלבים העיקריים של ביצוע הבחירות הכלליות. יש לקחת בחשבון כי בכל אחת מהחוליות בשרשרת עשויה להיות נקודת תורפה שתאפשר תקיפה.

א. הכנת הבחירות לכנסת

(**1**) הכנה במשרד הפנים של פנקס בוחרים מעודכן על בסיס המידע במרשם האוכלוסין,[92] בהתאם להוראות שבחוק הבחירות לכנסת.[93] בהתאם לחוק רק מי שרשום בפנקס הבוחרים רשאי להצביע לכנסת;[94]

(**2**) העברת פנקס הבוחרים ממשרד הפנים לוועדת הבחירות המרכזית;[95]

(**3**) אישור המפלגות הרשאיות להשתתף בבחירות ורשימת המועמדים לכל מפלגה,[96] ופרסום רשימות המועמדים לציבור;[97]

(**4**) קביעת אזורי הקלפיות וחלוקת הבוחרים לקלפי שבה הם רשאים להצביע.[98] לעניין זה קיימות הוראות מיוחדות לאפשרות לצרף קלפיות לפני יום הבחירות ומתן הודעה לבוחרים;[99]

(**5**) מינוי ועדות בחירות אזוריות[100] וועדות קלפי,[101] לרבות מזכיר ועדה לכל קלפי;[102]

(**6**) העברת רשימת הבוחרים שנקבעו לכל קלפי לידי מזכירי ועדות הקלפי;[103]

92 סעיף 29 לחוק הבחירות לכנסת [נוסח משולב], התשכ"ט–1969.

93 פרק ה' לחוק הבחירות לכנסת.

94 סעיף 2 לחוק הבחירות לכנסת.

95 סעיפים 39(ו) ו־71(א) לחוק הבחירות לכנסת.

96 סעיפים 57 ו־63 לחוק הבחירות לכנסת.

97 סעיף 65 לחוק הבחירות לכנסת.

98 בהתאם לסעיף 7 לחוק הבחירות לכנסת, למעט בוחרים מסוגים מיוחדים (חיילים למשל), לכל בוחר נקבעת קלפי קונקרטית בה הוא רשאי להצביע ורק בה.

99 סעיף 70 לחוק הבחירות לכנסת.

100 סעיף 20 לחוק הבחירות לכנסת.

101 סעיף 21 לחוק הבחירות לכנסת.

102 סעיף 21א לחוק הבחירות לכנסת.

103 סעיף 71 לחוק הבחירות לכנסת.

(**7**) העברת מידע מפנקס הבוחרים למפלגות – לרבות רשימת הבוחרים, אזורי הקלפי ומקומות הקלפי.[104] הפנקס מועבר למפלגות כ־50 ימים לפני מועד הבחירות;

(**8**) העברת הודעה לכל בוחר ששמו נכלל בפנקס הבוחרים בדבר כתובת הקלפי ששמו מופיע בה;[105]

(**9**) קביעת כינוי ואות ייחודי לכל רשימת מועמדים[106] ופרסום הרשימות והאותות;[107]

(**10**) הכנת פתקי ההצבעה[108] והעברתם לקלפיות;[109]

(**11**) ביצוע הכנות מיוחדות לעניין שוטרים הנמצאים בתפקיד ביום הבחירות, לרבות הנפקת תעודות הצבעה אישיות לשוטר ומחיקת אותם שוטרים מרשימת הבוחרים בקלפיות שבאזור מגוריהם;[110]

(**12**) הכנת הבחירות בכלי שיט והוראות לעניין ביצוע הבחירות בכלי שיט לפני יום הבחירות הכללי;[111]

(13) הכנת הבחירות בבתי כלא ובבתי מעצר;[112]

(**14**) הכנת הבחירות בנציגויות הדיפלומטיות והקונסולריות של ישראל, לרבות רשימת הזכאים להצביע;[113]

104 סעיף 39 לחוק הבחירות לכנסת.

105 סעיף 55ב לחוק הבחירות לכנסת.

106 סעיף 61 לחוק הבחירות לכנסת.

107 סעיף 65 לחוק הבחירות לכנסת.

108 סעיף 76 לחוק הבחירות לכנסת.

109 סעיף 77 לחוק הבחירות לכנסת.

110 סעיף 95 לחוק הבחירות לכנסת.

111 פרק י' לחוק הבחירות לכנסת.

112 סעיף 116ב לחוק הבחירות לכנסת.

113 סעיף 116ז ו־116י לחוק הבחירות לכנסת.

(**15**) הכנת הבחירות בבתי חולים ובמוסדות לאנשים המוגבלים בניידות, והוראות מיוחדות לעניין הרשאים להצביע בקלפיות בבתי חולים ובמוסדות לאנשים המוגבלים בניידות.[114]

ב. תהליך ההצבעה וניהול יום הבחירות לכנסת

(**1**) קביעת פרק הזמן שבו הקלפי פתוחה להצבעה;[115]

(**2**) קביעת הוראות לעניין אופן זיהוי הבוחרים;[116]

(**3**) קביעת סמכותם של ראש ועדת הבחירות המרכזית וסגניו לתת הוראות מיוחדות לקלפיות ספציפיות בערב יום הבחירות או ביום הבחירות, לרבות דחיית פתיחת הקלפי, הפסקת ההצבעה וחידושה וכן הוספת זמן להצבעה;[117]

(**4**) קביעת הסדרים מיוחדים לעניין הצבעת חיילים,[118] שוטרים וסוהרים;[119]

(**5**) קביעת הסדרים מיוחדים לעניין הצבעת בעלי תפקידים מיוחדים;[120] המוחזקים במשמורת הצבא[121] וימאים;

(**6**) קביעת הסדרים מיוחדים לעניין הצבעת אסירים, עצירים וסוהרים המצויים במשמרת;[122]

114 פרק י3 לחוק הבחירות לכנסת.

115 סעיף 72 לחוק הבחירות לכנסת.

116 סעיף 74 לחוק הבחירות לכנסת.

117 סעיף 70א לחוק הבחירות לכנסת.

118 סעיפים 89–91 לחוק הבחירות לכנסת.

119 **שם**.

120 סעיף 95א לחוק הבחירות לכנסת.

121 סעיף 95ב לחוק הבחירות לכנסת.

122 סעיפים 116ג ו־116ד לחוק הבחירות לכנסת.

(**7**) קביעת הסדרים מיוחדים לעניין ביצוע ההצבעה בנציגויות הדיפלומטיות והקונסולריות של ישראל;[123]

(**8**) קביעת הסדרים מיוחדים לעניין הצבעה בבתי חולים ובמוסדות לאנשים המוגבלים בניידות;[124]

ג. ספירת הקולות וקביעת תוצאות הבחירות

(**1**) הצבעה בפתק בלבד בתוך מעטפה המוטלת לקלפי לעיני ועדת הקלפי.[125] חלוקת מעטפה אחת לכל בוחר שהגיע לקלפי;[126]

(**2**) ספירת הקולות על ידי ועדת הקלפי[127] מייד לאחר תום ההצבעה ורישום פרוטוקול, לרבות הקולות שנפסלו;[128]

(**3**) העברת הקלפי והפרוטוקול לוועדת הבחירות האזורית;

(**4**) בדיקה של ועדת הבחירות האזורית את הרישומים שנעשו בוועדת הקלפי ותיקונם במידת הצורך.[129] צירוף פרוטוקול של ועדת הבחירות האזורית לפרוטוקול ועדת הקלפי;[130]

(**5**) העברת חומר הבחירות והפרוטוקולים לוועדת הבחירות המרכזית;[131]

123 סעיפים 116ח ו־116ט לחוק הבחירות לכנסת.

124 פרק י3 לחוק הבחירות לכנסת.

125 סעיף 75 לחוק הבחירות לכנסת.

126 סעיף 74א לחוק הבחירות לכנסת.

127 סעיף 79א לחוק הבחירות לכנסת.

128 סעיף 78 לחוק הבחירות לכנסת.

129 סעיף 79(ה)–(ז) לחוק הבחירות לכנסת

130 סעיף 79(ד) ו־79(ז) לחוק הבחירות לכנסת.

131 סעיף 79(ג) לחוק הבחירות לכנסת.

(6) ספירה של הקולות הכשרים מכל הקלפיות – הן מוועדות הקלפי הגיאוגרפיות והן מוועדות הקלפי המיוחדות – חלוקת המנדטים ופרסום תוצאות הבחירות על ידי ועדת הבחירות המרכזית.[132]

ד. הוראות לעניין שמירת מסמכים לרבות חומר הקלפי

בחוק נקבעו הוראות לעניין שמירת מסמכים, לרבות פרוטוקולים וחומר הקלפי למועדים המאפשרים אחזור החומר ובדיקתו.[133]

ה. מערכת המחשוב התומכת בניהול הבחירות

1. הכנת קובץ פנקס הבוחרים

כאמור, הפנקס נגזר ממערכת מרשם האוכלוסין וכולל את רשימת האזרחים בעלי זכות ההצבעה. תהליך הכנת הפנקס הוא באחריות משרד הפנים (מערכת "אביב"[134]).

2. מערכת מחשוב מרכזית לניהול הבחירות

מערך המחשוב שמשמש את ועדת הבחירות המרכזית מתבסס על מערך מחשוב עצמאי, מנותק ממערכות חיצוניות ומהאינטרנט, שנקרא "מערכת דמוקרטיה".[135] את המערכת פיתחה ומתחזקת חברה חיצונית, והשרתים מצויים אצלם בהנחיות אבטחה חמורות. ועדת הבחירות המרכזית – באחריות ראש אגף מחשוב ויועץ מחשוב שהיא מעסיקה – מבקרת את פעולות החברה, והיא שמפרסמת את ההנחיות בעניין המערכת.

3. מערכות מחשביות תומכות נוספות

נוסף על מערכת "דמוקרטיה", הוועדה מפעילה גם מערכות מחשביות נוספות, העיקריות שבהן הן מערכות השיבוץ של נציגי ועדת קלפי והוצאת כתבי המינוי.

132 סעיף 84 לחוק הבחירות לכנסת.

133 סעיף 79א לחוק הבחירות לכנסת.

134 דוח מבקר המדינה 66א בנושא ועדת הבחירות המרכזית (2015) עמ' 1874.

135 **שם**, בעמ' 1871.

מערכות אלה מתנהלת כחלק ממערכת שנקראת "ממשל זמין", פרי פיתוחן של חברות חיצוניות, ועל הפעלתה אחראי מערך המחשוב הממשלתי (יה"ב/תהיל"ה). חברות אלה חייבות לעמוד בתקן אבטחת המידע שקבע תהיל"ה, ולעבוד לפיו.

לסיכום, אחד השלבים העיקריים בתהליך הבחירות הוא ההכנה של רשימת בעלי זכות ההצבעה הנכללת בפנקס הבוחרים. פנקס הבוחרים הוא הרשומה העיקרית ומאגר המידע החשוב ביותר לקיום הבחירות, ועל פי החוק הוא מועבר לשימושה של ועדת הבחירות המרכזית וכן המפלגות. הכנת פנקס הבוחרים היא באחריות משרד הפנים, ופגיעה בו עלולה לשבש ואף למנוע את קיום הבחירות במועדן. זיופו עשוי להביא לידי הכללת מי שאינם זכאים להצביע בבחירות, או לגרוע כאלה הזכאים לכך. שיבוש או זיוף של פנקס הבוחרים עלולים, בסבירות גבוהה, לפגוע בתהליך הבחירות, ובסבירות נמוכה יותר להטות את תוצאותיהן.

בישראל מנהל את התהליך המרכזי, ההצבעה עצמה, גורם אחד – ועדת הבחירות המרכזית – והיא שאחראית על אבטחתו על כל שלביו. הבחירות מתבצעות על ידי הצבעה של בעלי זכות הבחירה בפתק נייר, שנשמר ומאפשר אחזור של ספירת הקולות בכל קלפי וקלפי. מערכות המחשב התומכות בתהליך (מערכת "דמוקרטיה" ומערכות מחשב נוספות) הן מערכות חיוניות לניהולה התקין של מערכת הבחירות. לפיכך פגיעה אפשרית במערכות אלה עלולה בסבירות גבוהה לשבש את ביצוע הבחירות, ובסבירות נמוכה יותר לזייף את תוצאותיהן.

2.
מפלגות ושחקנים פוליטיים: אפשרויות הפגיעה

א. מפלגות פוליטיות

מפלגות פוליטיות הן המסגרות החשובות ביותר בתהליך הבחירות בישראל, בעיקר לאחר ביטול הבחירה האישית לראש ממשלה. ההצבעה לכנסת היא

לרשימות מועמדים בלבד, קרי ־ למפלגות. מפלגות פוליטיות הן תאגידים,[136] כלומר גופים בעלי אישיות משפטית, וחלות עליהן הוראות מיוחדות מכוח חוק המפלגות. מטרתן העליונה של מפלגות פוליטיות היא להצליח להשיג את מרב הקולות מציבור הבוחרים, כדי לממש את סדר היום הפוליטי שלהן, ולשם כך הן פועלות בעיקר לקראת הבחירות.

מפלגות פוליטיות שוקדות כל ימות השנה על התכוננות לבחירות בהיבטים שונים, ובעיקר – הכנה ותחזוקה של רשימות התומכים והמתלבטים וביצוע פריימריז (במפלגות המפעילות בחירות מוקדמות). התקופה הרגישה שבה מפלגות פוליטיות מתכוננות לבחירות מתחילה במועד ההכרזה על בחירות, כלומר בין 150[137] ל־90 ימים לפני בחירות. מובן כי יום הבחירות עצמו הוא מועד רגיש במיוחד, שכן בו מופעלים מערכים מיוחדים, מבוססי מחשב, כדי להשיג את מרב הקולות.

באחדות מהמפלגות ניהול הפעילות הפוליטית – לרבות רשימות התומכים, המתלבטים, המתנדבים והפעילים – מתבצע במערכת מחשב ייעודית שמתוחזקת כל העת. המאגר כפוף להנחיות המצויות בתקנות לעניין ניהול ושמירת מאגר המידע[138] – בהיבטי הגנה על הפרטיות, שפרסמה הרשות להגנת הפרטיות במשרד המשפטים.

מתוך הראיונות שקיימנו עולה כי ככלל בכל הנוגע לאבטחת המידע במפלגה יש שונות גדולה בין המפלגות, מעצם היותן אוטונומיות ובהיבט זה לא כפופות לרשויות המדינה. אחדות מהמפלגות משקיעות במערכות אבטחה – לרבות עריכת סקרי סיכונים – יותר מהאחרות. זאת ועוד, לפחות באחדות מהמפלגות אבטחת המידע אינה חלה על המידע שברשותם של חברי הכנסת והעוזרים הפרלמנטרים. אחדות מהמפלגות רואות היבט זה באחריות קצין הכנסת, שכן התכתבויות הדואר האלקטרוני של חברי הכנסת ועוזריהם הפרלמנטרים מתבצעות מהשרתים של הכנסת.

136 סעיף 13 לחוק המפלגות, התשנ"ב–1992.

137 אם הבחירות מתקיימות במועדן החוקי – ראו סעיף 39(א) לחוק הבחירות לכנסת.

138 ראו הרשות להגנת הפרטיות/ בקשה לרישום מאגר מידע (אתר השירותים והמידע הממשלתי).

הסיכונים העיקריים לפגיעה במפלגות פוליטיות ובשחקנים פוליטיים באמצעות תקיפת סייבר הם:

1. פגיעה בבחירות המקדימות (פריימריז)

מפלגות שמקיימות בחירות מקדימות, ריבוניות להחליט על אופן ביצוע הבחירות בכפוף להוראות החוק, הנוגעות בעיקרן להגבלות על מימון הבחירות המקדימות למועמד ולענייני בקרה ודיווח למבקר המדינה. ברוב המפלגות המקיימות בחירות מקדימות, הבחירות מתבצעות באמצעות הצבעה ממוחשבת. בדרך כלל די בכמה אלפי קולות כדי להשפיע מהותית על תוצאות הבחירות המקדימות, ובכך על הרכב הרשימה לכנסת. תהליך הפריימריז הוא אפוא תהליך פגיע.

2. פגיעה ברשימת התומכים והמתלבטים או גנבתה

מפלגות פוליטיות זכאיות, לפי החוק, לקבל מידע על הבוחרים מפנקס הבוחרים.[139] רוב המפלגות משקיעות מאמץ רב לפלח את רשימת הבוחרים לרשימות תומכים ומתלבטים. חלק חשוב בהכנת מערכת הבחירות הוא בפנייה ממוקדת לקהל התומכים, כדי לשמרו, להמריצו לפעולה, לוודא שיגיע להצביע בפועל ולגייס מתוכו מתנדבים. אחדים מהמרואיינים ראו במאגר המידע המפולח את "הסוד הגדול" של ניצחון בבחירות, ואכן המפלגות משקיעות בכך מאמצים ומשאבים רבים. חשיבות מיוחדת יש גם לרשימת המתלבטים ובהעברת מסרים אליהם כדי להעבירם לרשימת התומכים. פגיעה במפלגה פוליטית באמצעות היזק, מניעת שימוש (DDOS) או זיוף של רשימת התומכים והמתלבטים והפרטים הרלוונטיים הנכללים בהן עלולה לפגוע במידה ניכרת ביכולתה של מפלגה להצליח בבחירות.

3. גנבה של אסטרטגיית הקמפיין לבחירות ושימוש מזיק בה

אסטרטגיית המפלגה לבחירות היא מהלך שבו רכיבים רבים, ובראש ובראשונה הנושאים שהמפלגה רוצה להבליט לקראת הבחירות ושעליהם ייסוב הדיון

139 סעיף 39(א) לחוק הבחירות לכנסת.

הציבורי כגון סוגיית השטחים, שחיתות שלטונית, כלכלה או איראן. מכאן שהאסטרטגיה של מפלגה כוללת את המסרים העיקריים שלה במערכת הבחירות. עוד נדבך חשוב באסטרטגיית בחירות הוא המסרים והמהלכים לפגיעה באסטרטגיה של מפלגות יריבות, במובן של "את מי תוקפים, מה תוקפים, ואיך תוקפים". אסטרטגיית הבחירות כוללת גם רכיבים כמו "הפתעות" וגימיקים, סיסמאות, עיצוב ולוגו, ג'ינגל הבחירות ועוד. מכאן שידיעת מהלכי הקמפיין עשויה לתת למפלגה יריבה יתרון ניכר, הן בהתכוננות למהלכי הקמפיין והן בנטרול מסרים ובהכנת מענה יעיל למהלכיו.

בהכנת קמפיין הבחירות עוסקים בדרך כלל כמה בכירי מפלגה וחברות לניהול קמפיינים, חברות פרסום ולעיתים גם יועצי בחירות עצמאיים. המשמעות היא כי המידע על אסטרטגיית הקמפיין מצוי אצל עשרות אנשים, שרובם מרוכזים במטה המפלגה, וכן אצל החברות הקובעות למפלגה את תוכני הבחירות, לרבות חברות פרסום. לפיכך חשוב מאוד למפלגה להגן על מחשביה שלה, על מחשביהם של האנשים המעורבים בקמפיין במפלגה ובחברות הקשורות, וכן על מכשירי הטלפון הניידים שלהם.

4. פגיעה במערכת הכספים של המפלגה או גנבת פרטים

ניהול קמפיין בחירות של מפלגה פוליטית, על כל הכרוך בכך, הוא עניין יקר שמושקעים בו סכומי כסף גדולים – חלקם מגיע מהמדינה בהתאם לחוק מימון מפלגות; וחלקם מתרומות. ההתנהלות הכספית של מפלגה ושל גופים שקשורים אליה[140] היא עניין בעל רגישות ציבורית יתרה, שמצוי בביקורת של מבקר המדינה.[141] גם רשימת התורמים למפלגה היא נושא בעל רגישות ציבורית, בוודאי בתקופת הבחירות. גנבה של פרטי המערכת הכספית והדלפתה עלולה להעמיד את המפלגה במצב מביך ולהציב אותה בעמדת מגננה, בייחוד אם דליפה כזאת מתבצעת בשלב קריטי של הקמפיין.

140 גוף הקשור לסיעה (סעיף 10א לחוק מימון מפלגות) וגוף הפעיל בבחירות (סעיף 10ג לחוק מימון מפלגות).

141 סעיף 10 לחוק מימון מפלגות.

5. גנבה והדלפה של מידע על הסכמים ומגעים פוליטיים

בריתות פוליטיות, אד הוק או מעבר לכך, וכן מגעים עם אישים להצטרפות או להבעת תמיכה פומבית במפלגה הם חלק בלתי נפרד מקמפיין פוליטי. מגעים אלה נשמרים בדרך כלל בסוד עד המועד שבו ראשי המפלגה מחליטים כי חשיפתם תספק את התמורה הציבורית המרבית. דליפה מוקדמת עלולה לטרפד מגעים כאלה או לפגוע ברווח הפוליטי המקווה. למפלגה יש אפוא אינטרס מובהק שמגעים אלה יישמרו בסוד עד המועד שבו יוחלט לחשוף אותם, וגנבתם ודליפתם בטרם עת עשויים לסייע ליריביהם הפוליטיים.

6. פגיעה בארגון הלוגיסטי של המפלגה ליום הבחירות

יעד עיקרי של המפלגה הוא לוודא כי תומכיה מגיעים לקלפי כדי להצביע בפועל. לעניין זה חשיבות רבה ביום הבחירות. לשם כך המפלגות מתבססות על רשימות תומכים ומתלבטים, לרבות פרטי הקשר הטלפוני עמם, וביום הבחירות מפעילות מערכת של התקשרויות בטלפון וכן מערך היסעים למצביעים הזקוקים לכך. ארגון המפלגה לקראת יום הבחירות מבוסס בין היתר על מערכות מחשב שכוללות את רשימות הפעילים המועסקים במפלגה ביום הבחירות, בשכר או בהתנדבות ותיאור תפקידיהם, רשימת המטות האזוריים שהמפלגה מפעילה, מיקומם, אופן פעולתם והיבטים לוגיסטיים שנוגעים להפעלתם. שיבוש המערכת הארגונית של המפלגה ליום הבחירות עלול לפגוע במידה ניכרת במספר הקולות שהמפלגה תקבל בפועל.

ב. שחקנים פוליטיים

גם שחקנים פוליטיים הם יעד חשוב להשפעה, שכן פגיעה בהם באמצעות התקפות סייבר עלולה להשפיע על תוצאות הבחירות. שחקנים כאלה הם למשל חברי כנסת מכהנים, מועמדים לחברי כנסת, שרים ואישים בולטים במפלגות. לאחדים מאישים אלה יש עוזרים פרלמנטרים או עוזרים פוליטיים אחרים, ואצלם מופקדים עניינים רגישים שפרסומם עלול להביך את המועמדים. בכנסת לבדה מדובר בכמה מאות אנשים (בכנסת 120 חברי כנסת מכהנים, ולכל אחד מהם כשלושה עוזרים פרלמנטרים). לאחדים מאישים אלה נוכחות ברשת –באתר

אישי או ברשתות החברתיות – פייסבוק, טוויטר, אינסטגרם וכדומה, ערוצים שבהם מתקיים קשר בינם לבין הציבור. שחקנים פוליטיים עלולים להיות פגיעים להתקפות סייבר בכמה היבטים:

1. גנבה והדלפה של מידע המצוי בתכתובת אישית

התכתבויות אישיות – בעיקר בנושאים פוליטיים או עם שחקנים פוליטיים אחרים – עשויות לכלול מידע שהדלפתו עלולה להביך את מי שהמידע נגנב ממנו, אם בתוכן – למשל מגעים פוליטיים חשאיים שהוא מנהל; ואם בסגנון – בשפה בוטה על יריבים ולעיתים על עמיתים וכדומה. התכתובת האישית מתנהלת בהתאם להחלטותיו של כל שחקן – בכתובת דוא"ל של המפלגה או של הכנסת; בתכתובת דוא"ל אישית; ולעיתים בכמה כתובות שיש להן מאפיינים שונים. התכתבויות נעשות גם באמצעות מסרונים בטלפון הנייד – SMS, הודעת ווטסאפ או תוכנת העברת מסרים אחרת.

2. פגיעה באתר פוליטי־אישי

פגיעה באתר אישי ברשת או בחשבון המתנהל ברשת חברתית כגון פייסבוק או טוויטר, עשויה להיעשות אם על ידי שיבוש ו"הפלת" אתר; ואם על ידי שתילת מידע כוזב, בתגובות (טוקבקים) של מגיבים מוטים בשכר (טרולים), טוקבקים מזויפים ועוד.

ג. מניפולציה על דעת הקהל בישראל

רובם המכריע של הישראלים משתמשים באינטרנט. לפי נתוני איגוד האינטרנט בישראל בשנת 2017 גלשו יותר מ־90% מהישראלים באינטרנט –במחשב, בטלפון הנייד או במחשבי לוח (טאבלט)[142] – ושיעור ניכר (63%) השתמש גם ברשתות חברתיות. מנתונים אלה עולה עוד כי רבים מהמשתמשים (75%) צורכים את החדשות מהאינטרנט, רובם מאתרי חדשות בעברית (66% מהמשתמשים), ו־7%

142 הגולש הישראלי – פערים בשימוש באינטרנט במגזר היהודי והערבי (אתר איגוד האינטרנט הישראלי, יוני 2017).

מהאוכלוסייה מסרו כי הם צורכים את החדשות מרשתות חברתיות.[143] מנתוני הסקר עולה עוד כי 6% מהאוכלוסייה צורכים את החדשות מאתרי חדשות בערבית (36% מהגולשים הערבים), ו־3% מהאוכלוסייה צורכים חדשות מאתרים בשפה הרוסית. מנתונים שאספה חברת בזק בשנת 2017 עולה תמונה דומה: כ־62% ממשתמשי האינטרנט דיווחו כי צרכו חדשות מאתרי חדשות באינטרנט, ואילו 48% דיווחו כי צרכו חדשות מרשתות חברתיות, לעומת 40% בלבד שדיווחו כי צרכו חדשות ממהדורות החדשות בטלוויזיה.[144]

מהנתונים גם עולה כי מקרב הרשתות החברתיות, ווטסאפ היא האפליקציה בשימוש הרב ביותר בכל הגילים. מספר המשתמשים באינסטגרם עבר, בקרב בני נוער, את מספר המשתמשים בפייסבוק, אבל בקרב מבוגרים יותר הפייסבוק מוביל ללא עוררין.[145] 36% ממשתמשי הפייסבוק ציינו כי הם משתמשים ברשת כמקור לצריכת חדשות.[146] מהרגלי שימוש אלה עולה בבירור שהרשת היא מקור השפעה פוטנציאלי חשוב על עיצוב תודעת הבוחרים הישראלים, הן דרך אתרי חדשות והן דרך רשתות חברתיות.

בכל הנוגע להתמודדות עם מניפולציה דרך אתרי חדשות ורשתות חברתיות קיים קושי מובנה, שמקורו בשני היבטים עיקריים: ראשית, הבחנה לא ברורה בין מידע כוזב שהוא חלק מחופש הביטוי; ובין מידע זדוני, בוודאי אם הוא חלק ממבצע השפעה שמנהלת ישות זרה, שמצדיק בעיקרון התערבות מדינתית.[147] שנית, גם כשאפשר להבחין בין סוגי המידע (בין הלגיטימי ללא לגיטימי בתחום המניפולציה בדעת הקהל), יש לבחון באילו כלים אפשר להשתמש כדי להתמודד

143 שם.

144 החיים בעידן הדיגיטלי: דוח האינטרנט של בזק 2017 (להלן: סקר בזק 2017).

145 שם.

146 שם.

147 "לא ברור האם וכיצד יש להתמודד עם סוגיית ההפצה של מידע כוזב, ומהו התפקיד של המדינה בעניין או חלקם של שחקנים אחרים דוגמת גופי תקשורת או גופי מגזר שלישי. נראו כי אין כיום כלים מספקים כדי לאמוד את מידת ההשפעה של מידע כוזב על מערכות בחירות", ראו רועי גולדשמיט "הפצת מידע כוזב באינטרנט ותקיפות סייבר לשם השפעה על בחירות" (מרכז המחקר והמידע של הכנסת, 11.6.2017).

עם מניפולציה כזאת – כלים חוקיים, רגולטוריים או אחרים כגון חשיפת המניפולציה לציבור. כמו כן לא ברור איזה גורם מופקד על האיתור והניטור של המניפולציה ברשת, על הפעולה למניעתה או על נטרול השפעתה.

לסיכום, תהליך הבחירות בישראל עלול להיות יעד לתקיפת סייבר בשלוש זירות התקיפה שנסקרו. הזירה הראשונה היא ביצוע הבחירות – שאף שהוא מבוסס על הצבעה באמצעות נייר, נתמך במערכות מחשביות משלב ההכנה של פנקס הבוחרים ועד חישוב התוצאות ושקלולן. מערכות אלה עלולות להיות יעד לתקיפת סייבר. הזירה השנייה היא המפלגות והשחקנים הפוליטיים, העלולים להיות יעד לתקיפה; והזירה השלישית היא הרשתות החברתיות, שבניסיון להשפיע על הבחירות באמצעות מניפולציות על דעת הקהל עלולות להיות גם הן יעד לתקיפה של ישות זרה. לנוכח לקחי התקיפות במדינות אחרות, הגנה של זירות אלה מצריכה גיבוש תפיסה שמותאמת למצב בישראל וטעונה טיפול מערכתי מקיף. בתת־הפרק הבא ייסקרו הגופים האמונים כיום על הגנת תהליך הבחירות בישראל.

פרק ג
המערכת המוסדית המופקדת על הגנת תהליך הבחירות מפני התקפות סייבר והסביבה המשפטית שבתוכה היא פועלת

תקיפות סייבר במטרה לפגוע בתהליך הבחירות בישראל עלולות להתבצע בכל הדרכים שבהן הותקפו מערכות בחירות בעולם – בין היתר באמצעות פגיעה ברכיבים חיוניים; מחיקה של מידע; שיבוש ומניעת גישה לשירות (DDOS); פריצה וגנבה מרחוק של מידע ושימוש בו לפגיעה במערכת או ביריב פוליטי; זיוף או שתילה של מידע כוזב; הטיית שיח ומניפולציה של תכנים; ושימוש בחשבונות פיקטיביים. כל דרך כזאת, ובוודאי שילוב של כמה דרכים שמופעלות באפקטיביות, עלולה להשפיע על תוצאות הבחירות ולהביא לידי פגיעה באמון הציבור בתוצאותיהן. בפרק זה נבחן מיהם הגופים שבאחריותם להגן על תהליך הבחירות ומהם הרכיבים המשפטיים הרלוונטיים המגדירים את אחריותם ואת סמכויותיהם.

1. ועדת הבחירות המרכזית: אחריות וסמכויות

ועדת הבחירות המרכזית לכנסת מוקמת מכוח חוק הבחירות לכנסת.[148] זו ועדה סטטוטורית קבועה, שפועלת בכל ימות השנה. הודעה על הרכב הוועדה נמסרת לכנסת ומפורסמת ב"רשומות".[149] הרכב הוועדה מוחלף בתוך 60 יום מכינוסה

148 סעיף 15 לחוק הבחירות לכנסת (נוסח משולב), התשכ"ט–1969.

149 סעיף 23 לחוק הבחירות לכנסת.

של כנסת חדשה.[150] בראש הוועדה עומד שופט בית המשפט העליון, שבית משפט זה בוחר בו לתפקיד.[151] לצד ועדת הבחירות פועל בקביעות סגל מינהלי שמופקד על ההיערכות לבחירות ועל ניהולן, ובראשו מנכ"לית ועדת הבחירות. במסמך זה אנו עוסקים באחריות ובתפקידים הן של יושב ראש הוועדה והן של הסגל המינהלי, שתפקידו המרכזי הוא ביצוע הבחירות.[152]

על פי החוק תפקידה של ועדת הבחירות המרכזית לדאוג "לביצוע הבחירות".[153] מכאן שהיא אחראית לביצוע הבחירות על כל היבטיהן הלוגיסטיים והתהליכיים הקבועים בחוק הבחירות לכנסת להכנת הבחירות ולמימושן, לרבות ניהול יום הבחירות, ספירת הקולות הכשרים, פרסום התוצאות ושמירת חומר הבחירות לשם בדיקה של ערעורי בחירות.

לשם מילוי תפקידה ניתנו לוועדת הבחירות מגוון של סמכויות, לרבות תקציב[154] וסמכות להתקשר בחוזים לשם ביצוע עסקאות.[155] נוסף על הסמכויות הקונקרטיות, נקבעה בחוק הוראה כללית שלפיה "כל משרדי הממשלה והרשויות המקומיות יגישו את העזרה שתדרוש מהם הועדה המרכזית".[156] כדי להצליח במשימתה מקיימת ועדת הבחירות המרכזית שלד ארגוני קבוע שכולל כ־30 איש, מקצתם בחלקיות משרה. לקראת בחירות עולה מספרם לכ־1,000 איש, וביום הבחירות עצמו מעסיקה הוועדה כ־50,000 איש. מדובר במבצע לוגיסטי מורכב מאוד, בלוח זמנים מוכתב וקבוע (90 ימים בדרך כלל), שמחייב תחזוקה, התכוננות והיערכות מקצועית ולוגיסטית כל העת. בשל פרק הזמן

150 **שם**, סעיף 15(א).

151 סעיף 17 לחוק הבחירות לכנסת.

152 מבקר המדינה, דוח שנתי 66ג – לשנת 2015, בעמ' 1816.

153 סעיף 15(א) לחוק הבחירות לכנסת.

154 סעיף 134א לחוק הבחירות לכנסת.

155 סעיף 25א לחוק הבחירות לכנסת.

156 סעיף 150 לחוק הבחירות לכנסת.

הקצר וההיערכות הרבה הנדרשת, מחזיקה הוועדה מחסן לוגיסטי מרכזי ובו הציוד הנדרש.[157]

מאגר המידע המרכזי המשמש לביצוע הבחירות הוא כאמור פנקס הבוחרים. את פנקס הבוחרים מקבלת ועדת הבחירות המרכזית לידיה ממשרד הפנים,[158] לפי דרישת הוועדה ובמועדים הקבועים בחוק.[159] הפנקס כולל את פרטיהם האישיים של בעלי זכות הבחירה לרבות מענם הרשום, ואת חלוקת בוחרים לפי אזורי הבחירה שבהם מוצבות קלפיות.

נוסף על התפקיד והסמכויות הנוגעים לביצוע הבחירות לפי חוק הבחירות, נמסרו ליושב ראש ועדת הבחירות המרכזית סמכויות נרחבות גם לפי חוק הבחירות לכנסת (דרכי תעמולה) (להלן: חוק דרכי תעמולה).[160] חלק מהוראותיו של חוק דרכי תעמולה חלות בתקופת 90 הימים שלפני מועד הבחירות לכנסת, וחלק מהוראותיו חלות בלי קשר למועד הבחירות.[161] כך למשל האיסור על מפלגה או על מי מתומכיה להפריע הפרעה "בלתי הוגנת" לתעמולת בחירות של מפלגה אחרת חל בכל ימות השנה.[162]

ההוראות העיקריות לעניין תעמולת בחירות חלות בתקופה של 90 הימים שלפני מועד הבחירות וכן ביום הבחירות עצמו. בין היתר חלות ההוראות לעניין חובת ייחוס מודעת בחירות למזמין המודעה, לרבות אם הוא מטעם מועמד או מפלגה,[163] והוראות מיוחדות לעניין פרסום סקר בחירות, בייחוד בשבוע האחרון

157 שיחה עם עו"ד דין לבנה – היועץ המשפטי לוועדת הבחירות המרכזית.

158 סעיף 71(א) לחוק הבחירות לכנסת.

159 סעיפים 39(ו) ו־(ז) לחוק הבחירות לכנסת.

160 חוק הבחירות לכנסת (דרכי תעמולה), התשי"ט–1959; לעניין תיחום היקף שיקול הדעת של יושב ראש ועדת הבחירות לעניין הוצאת צווי מניעה בהתאם לחוק הבחירות לכנסת (דרכי תעמולה) לגדרי הוראות 17ב(א) לחוק – ראו גם דנג"צ 1525/15 **ח"כ ד"ר אחמד טיבי נ' מפלגת ישראל ביתנו ואח'** (2017).

161 סעיף 2 לחוק דרכי תעמולה.

162 סעיף 13 לחוק דרכי תעמולה.

163 סעיפים 10(א)(3), 10(ב)(5) ו־10א לחוק דרכי תעמולה.

שלפני מועד הבחירות.[164] זה הסעיף היחיד בחוק דרכי תעמולה שבו קיימת התייחסות מפורשת לפרסום באינטרנט.[165]

חוק דרכי תעמולה מטיל סנקציות פליליות על הפרת הוראה מהוראות חוק זה או על הפרת חיוב שהטיל מכוח החוק יושב ראש ועדת הבחירות המרכזית.[166] החוק גם מקנה ליושב ראש הוועדה את הסמכות להוציא צו מניעה במטרה למנוע ביצוע עבירה על חוק דרכי תעמולה או על חוק הבחירות לכנסת,[167] ואם הופר צו המניעה, רשאי היושב ראש להטיל על המפר קנס לפי פקודת ביזיון בתי המשפט.[168]

השאלה אם סמכותו של יושב ראש ועדת הבחירות המרכזית לתת צווי מניעה משתרעת גם על פרסומים ברשת האינטרנט לא הוכרעה בברור: בפסק דין שניתן בשנת 2001 קבע השופט חשין כי מאחר שלא נקבע בחוק איסור מפורש על תעמולת בחירות באינטרנט, אזי בשל חשיבות חופש הביטוי אין לקרוא לחוק סמכות שלא כתובה בו – לאסור על תעמולה כאמור – ומכאן שאין סמכות להוציא צווי מניעה כמו שהתבקש בעתירה.[169] בהסתמך על אותם טעמים דחתה השופטת ביניש, בהחלטה נוספת משנת 2006, בקשה לאסור על פרסום מודעת בחירות באינטרנט.[170]

בשנת 2013, בשל מרכזיותו של המרחב המקוון גם בעניין תעמולת בחירות, השתנתה המגמה. השופט רובינשטיין, שכיהן כיושב ראש ועדת הבחירות באותו מועד, לא נמנע מלהידרש לתלונות בנושא פרסומים ברשת וברשתות חברתיות,[171]

164 סעיף 16(ה) לחוק דרכי תעמולה.

165 סעיף 16ה(א) לחוק דרכי תעמולה.

166 סעיפים 17 ו־17א לחוק דרכי תעמולה.

167 סעיף 17ב לחוק דרכי תעמולה.

168 סעיף 17ב(ג) לחוק דרכי תעמולה.

169 השופט חשין בתב"מ 16/01 **ש"ס התאחדות הספרדים נ' ח"כ אופיר פינס** (2001).

170 תב"כ 3/17 **אמיר לירן נ' חברת רוטר.נט בע"מ** (2006).

171 ועדת הבחירות המרכזית לכנסת השע־עשרה החלטות והנחיות ממערכת הבחירות לכנסת ה־19 וממערכת הבחירות לרשויות המקומיות 2012־2013, בעמ' 193–195. וכן

ובמסמך הלקחים שחיבר בעקבות הבחירות התייחס מפורשות לעניין זה: "אציין כי לא ראיתי, שלא כפסיקה קודמת ותפיסתי שלי בתחילה, לפטור את האינטרנט מתחולת חוק דרכי תעמולה, וזאת כדי שלא להפוך את החוק, עם ההתפתחויות הטכנולוגיות, לחוכא ואיטלולא".[172] גם בהחלטות מאוחרות יותר סברו יושבי ראש ועדת הבחירות כי יש בידם סמכות עקרונית להוציא צווים גם בנוגע לפרסומים באינטרנט. עד כה טרם הוסדר עניין זה מפורשות בחוק.[173]

בעקבות השינויים שחלו במציאות התקשורתית והפוליטית מאז שנחקק חוק דרכי תעמולה בסוף שנות החמישים, נוצר קושי הולך וגובר לאכוף את האיסורים הנכללים בו. שינויים אלה הביאו לכך שנוצר בחוק חסר עמוק ומהותי עד כדי ספק חמור ברלוונטיות שלו. ההתפתחויות הטכנולוגיות – ובראשן האינטרנט, הרשתות החברתיות והטלפונים הניידים – יצרו צורך חיוני בהתאמת החוק למדיום זה. לפיכך ובהתאם להמלצותיהם של יושבי ראש ועדת הבחירות שכיהנו במערכות הבחירות האחרות,[174] מונתה ועדה ציבורית בראשותה של נשיאת בית המשפט העליון בדימוס דורית בייניש במטרה לבחון את חוק דרכי תעמולה ולהציע הצעות לשינויו. דוח הוועדה הוגש בנובמבר 2017.

בעניין תחולת החוק על האינטרנט המליצה הוועדה "להחיל את הוראות החוק המהותיות גם באינטרנט וברשתות החברתיות. הסדרים כלליים בחוק יחולו על תעמולת בחירות בכל מדיום שהוא ובכל אקלים טכנולוגי ותקשורתי",[175] ובוודאי

דברי השופט רובינשטיין בחב"כ 16/19 **רשימת הבית היהודי בראשות נפתלי בנט נ' רשימת הליכוד ביתנו לכנסת ה־19 ואחי** (2013): "אין סיבה להבדיל, בהקשר סעיף 10(ב)(5) לחוק דרכי תעמולה, בין פרסומים בעיתונות ועל־גבי לוחות מודעות, לבין פרסומים באינטרנט" (פסקה ה).

172 **שם**, עמ' 522.

173 ראו דברי השופט ג'ובראן בתר"מ 177/20 **ח"כ עמר בר לב נגד נוימרק קורן ואח'** (2013); ובחב"כ 9/20 **פרופ' יוסי יונה ואחי נגד ח"כ נפתלי בנט יו"ר הבית היהודי ואחי** (2015).

174 הוועדה הציבורית לבחינת חוק הבחירות (דרכי תעמולה), התשי"ט–1959, **דין וחשבון** 7 (2017).

175 **שם**, בעמ' 34.

שאין מקום, לדעת הוועדה, להבחין בין פרסום באתר חדשות מקוון ובין פרסום ברשתות חברתיות כמו פייסבוק או טוויטר.[176]

בעקבות הגשת הדוח הכינה ועדת החוקה, חוק ומשפט של הכנסת הצעה (חלקית) לתיקון החוק.[177] על פי ההצעה ייקבע בחוק עקרון השקיפות וחובת הייחוס, כלומר שעל כל תעמולת בחירות מטעם מפלגה או תעמולה בתשלום (למעט פרסום על ידי אדם פרטי שלא בתשלום), יחתום מי שעומד מאחוריה כך שניתן יהיה ליחסה לגורם מזוהה, ועיקרון זה יחול גם על פרסומים באינטרנט. לפי ההצעה הוראה זו תחול תמיד, ולא רק לקראת בחירות, וכן תחול גם בבחירות מקדימות.[178]

מהאמור לעיל עולה כי לוועדת הבחירות המרכזית בכלל, וליושב ראש ועדת הבחירות המרכזית בפרט, ניתנה אחריות כוללת ומקיפה הן למימוש תהליך הבחירות בהתאם להנחיות שבחוקי הבחירות, והן למימוש הכללים הנוגעים לתעמולת בחירות, לרבות סמכויות אכיפה נרחבות, והוראות אלה כוללות גם את המרחב המקוון. מכוח אחריות כוללת זו הנחה המחוקק את רשויות המדינה להושיט לוועדת הבחירות המרכזית כל סיוע שיידרש כדי שתוכל לממש את ייעודה ואת תפקידיה.

בשל עצמאות הוועדה, לא נקבעה רשות אחרת המופקדת על הגנת הוועדה ופעולותיה מפני התקפות סייבר. מטעם זה הוועדה אינה כלולה ב"גופים המונחים" הנמנים בתוספות הרלוונטיות לחוק להסדרת הביטחון בגופים ציבוריים.[179] התוצאה היא שבאופן רשמי הוועדה אינה כפופה להנחיות של שירות הביטחון הכללי או מערך הסייבר הלאומי. עם זה, בעקבות הבנת הצורך בדבר הגנה מפני התקפות סייבר גובשו סיכומים לא פורמליים בין הוועדה ובין גופי אבטחת הסייבר, שבהם נקבע כי הוועדה תקבל על עצמה "באורח וולונטרי" הנחיות אבטחה בתחום זה. בעבר היו קשרי עבודה, רופפים למדי, בנושא בין

176 שם.

177 הצעת חוק הבחירות (דרכי תעמולה) (תיקון מס' 34), התשע"ח–2018, הצעות חוק הכנסת 805.

178 גיא לוריא ותהילה שוורץ־אלטשולר "רפורמה בדיני בחירות" (מחקר מדיניות 109, המכון הישראלי לדמוקרטיה, 2015).

179 חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998.

הוועדה ובין הרשות הממלכתית לאבטחת מידע שפעלה במסגרת השב"כ, אולם מאז הקמתו של מערך הסייבר הלאומי נעשה הקשר הדוק יותר.[180] בתוך הוועדה אחראי על הנושא מנהל מערכות המידע (מנמ"ר) שלה, והמערך העוסק בכך נמצא הולך ומתעבה

נראה כי בשל חשיבותו של תהליך הבחירות מזה והיקף האיומים בתחום הסייבר מזה, אין להותיר את ההסדר במתכונת של "הנחיה מרצון", ויש ליצור הגדרה פורמלית של האחריות והסמכויות של ועדת הבחירות המרכזית או יושב ראש ועדת הבחירות המרכזית בתחום הגנת מערכת הבחירות מפני איומי סייבר, כמו שיפורט להלן בפרק ההמלצות.

2. מערך הסייבר הלאומי: אחריות ותפקידים

מערך הסייבר הלאומי פועל מכוח כמה החלטות ממשלה.[181] בהתאם להחלטות אלה "הגנת סייבר" מוגדרת "מכלול הפעולות למניעה, לנטרול, לחקירה ולהתמודדות עם איומי סייבר ואירועי סייבר ולצמצום השפעתם והנזק הנגרם מהם, וזאת בטרם התרחשותם, במהלכם ולאחריהם".[182] עוד נקבע כי ההגנה על תפקודו התקין והבטוח של מרחב הסייבר היא יעד ביטחוני לאומי חיוני של

180 שיחות עם עו"ד דין לבנה – היועץ המשפטי לוועדת הבחירות המרכזית; יגאל אונא – ראש מערך הסייבר הלאומי; רפי פרנקו – ראש מכלול עמידות במערך הסייבר הלאומי.

181 החלטה 3611 של הממשלה ה־32 "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.2011) (להלן: **החלטת ממשלה 3611**); החלטה 2443 של הממשלה ה־33 "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.2015) (להלן: **החלטת ממשלה 2443**); החלטה 2444 של הממשלה ה־33 " קידום ההיערכות הלאומית להגנת הסייבר" (15.2.2015) (להלן: **החלטת ממשלה 2444**); החלטה 3270 של הממשלה ה־34 "(1)איחוד יחידות מערך הסייבר הלאומי; (2) מתן פטור ממכרז למשרת ראש מערך הסייבר הלאומי; (3) הוספת משרת ראש מערך הסייבר הלאומי לתוספת לפי סעיף 23 לחוק שירות המדינה (מינויים); (4) קביעת שכר ותנאי שירות של ראש מערך הסייבר הלאומי" (17.12.2017) (להלן: החלטת ממשלה 3270).

182 החלטות ממשלה 3611 ו־2444.

המדינה ואינטרס ממלכתי חיוני לביטחונה הלאומי. לפי החלטות הממשלה משנת 2015 הוקמו שני גופים – הרשות הלאומית להגנת הסייבר ומטה הסייבר הלאומי;[183] ואלה אוחדו בשנת 2017 לגוף אחד – מערך הסייבר הלאומי.[184] בהחלטה נקבע כי תפקידיו ויעדו של מערך הסייבר הלאומי יהיו בהתאם להחלטות הממשלה שהקימו את שתי היחידות שמהן הורכב המערך – הרשות והמטה.

כדי לעמוד על ייעודו ועל תפקידיו של מערך הסייבר הלאומי, יש לקרוא אפוא את החלטות ההקמה הן של הרשות להגנת הסייבר והן של מטה הסייבר הלאומי.

א. רשות הסייבר הלאומית

בהתאם להחלטת ממשלה 2444 מפברואר 2015, תפקידה העיקרי של הרשות הוא הגנת מרחב הסייבר הלאומי. בין יתר תפקידיה נמנים התפקידים האלה:

> (**2א**) לנהל, להפעיל ולבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית במרחב הסייבר, בתפיסה מערכתית, לטובת מענה הגנתי שלם ורציף למול תקיפות סייבר, ובכלל זה טיפול באיומי סייבר ובאירועי סייבר בזמן אמת, גיבוש תמונת מצב שוטפת, ריכוז ומחקר מודיעין, ועבודה עם הגופים המיוחדים [...]
>
> (**ב**) להפעיל מרכז לסיוע בהתמודדות עם איומי סייבר (להלן: **ה־CERT הלאומי**) עבור כלל המשק, ובכלל זה לפעול לשיפור החוסן ההגנתי בסייבר, לסייע בטיפול באיומי סייבר ואירועי סייבר, לרכז ולשתף מידע רלוונטי עם כלל הגורמים במשק ולהוות נקודת ממשק מרכזית בין גופי הביטחון לבין הגורמים במשק...
>
> (**ג**) לבנות ולחזק את החוסן של כלל המשק בסייבר באמצעות היערכות, כשירות ואסדרה, ובכלל זה העלאת הכשירות של מגזרים וגופים במשק, הנחיית המשק בתחום הגנת הסייבר, אסדרת שוק שירותי הגנת הסייבר, רישוי, תקינה, עריכת תרגילים ואימונים, מתן תמריצים וכלים נדרשים נוספים.

183 החלטות ממשלה 2443 ו־2444.

184 החלטת ממשלה 3270.

(**ד**) לעצב, ליישם ולהטמיע תורה לאומית להגנת הסייבר.

(**ה**) לבצע כל תפקיד אחר שיקבע ראש הממשלה בהתאם לייעוד הרשות.[185]

ב. מטה הסייבר הלאומי

על פי אותה החלטת ממשלה (2444) מפברואר 2015, ייעודו של מטה הסייבר הלאומי לקדם את המדיניות ואת האסטרטגיה בתחום הסייבר ברמה הלאומית, לטפל בבניין הכוח הלאומי ובחיזוקה של מדינת ישראל כמובילה עולמית בתחום הסייבר. בין יתר תפקידיו נמנים התפקידים האלה:

(**5**) להטיל על המטה להקים תשתית טכנולוגית וארגונית לאומית לגילוי, זיהוי, חקירה, התרעה ושיתוף מידע, לצורך גילוי וזיהוי של תקיפות סייבר על מדינת ישראל [...].

(**6**) להטיל על הגופים המיוחדים לעבוד עם הרשות לטובת הגנת הסייבר, כל אחד במסגרת הדין החל עליו ועל פיו ובהתאם לייעודו וסמכויותיו [...]

(**7**) להקים פורום הגנת הסייבר, בראשות ראש הרשות, שמטרתו תיאום, בקרה והסדרה של הפעילות המשותפת לרשות ולגופים המיוחדים [...]

(**8**) להנחות את משרד החוץ והרשות לפעול בתיאום, בשיתוף ובהתייעצות בהיבטים הרלוונטיים למול הזירה הבינלאומית, [...].[186]

החלטות ממשלה אלה הן המסדירות כיום את ייעודו ואת תפקידיו של מערך הסייבר הלאומי. ואולם ההבנה כי היקף האחריות של הגנת הסייבר והסמכויות הנדרשות למימושו מצריכים הסדרה בחקיקה ראשית הביאה לידי תהליך חקיקה שהחל עם פרסומו של תזכיר חוק הסייבר, שהופץ בשנת 2018 והועבר להתייחסויות לקראת הגשתו כהצעת חוק ממשלתית.[187]

185 סעיף 2 להחלטת ממשלה 2444.

186 **שם**, סעיפים 5–8.

187 תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח–2018 (להלן: תזכיר חוק הסייבר).

תזכיר חוק הסייבר נועד לקבוע בחקיקה ראשית את תפקידיו ואת סמכויותיו של מערך הסייבר הלאומי. כאמור בדברי ההסבר, מטרת החוק המוצע לעגן את החלטות הממשלה בדבר חקיקה ולקבוע כי מערך הסייבר הלאומי הוא:

> גוף ממשלתי שמשימתו הגנה לאומית בתחום הסייבר המבוססת על תחום טכנולוגיית המידע (מחשבים, רשתות והגנת הסייבר) תוך ביצוע פעילויות ביטחוניות, אופרטיביות ורגולטוריות, שתכליתן למנוע מהאיום להתממש.[188]

עוד מתפקידו של המערך להגן על תפקודו התקין של מרחב הסייבר ולמנוע תקיפות שיש בהן כדי לסכן במידה ניכרת את האינטרס הציבורי. מבחינה מעשית תפקידי המערך הם למנוע תקיפה, לאתר תקיפה, להכיל את הנזק ולסלק את התקיפה[189] – במקרים שבהם הארגון המותקף, בין שהוא פרטי ובין שהוא ציבורי, אינו מסוגל בעצמו לאתר את התקיפה במדויק או להתמודד עימה ולמנוע את הנזק מהאירוע.[190]

ההצעה שבתזכיר חוק הסייבר כוללת הוראות לעניין הגופים שישתתפו במערך הגילוי והזיהוי של התקפות סייבר. על פי ההצעה גופים אלה כוללים בין היתר "גוף מבוקר" – כהגדרתו בסעיף 9 לחוק מבקר המדינה, ובלבד שראש המערך קבע "ששיתופו יתרום תרומה של ממש לגילוי תקיפות סייבר".[191] מאחר שוועדת הבחירות המרכזית היא "גוף מבוקר" כאמור,[192] לכאורה, בהתאם להצעת החוק שבתזכיר, לא מן הנמנע להכליל אותה בגופים שיהיו חלק ממערך הגילוי והזיהוי של התקפות סייבר.

התפיסה שבבסיס ההצעה היא מערכתית, לאמור, היא מתבססת על שיתוף מידע בין ארגונים, לרבות מידע שמקורו בארגוני הביטחון, לשם גילוי וזיהוי של

188 **שם**, בעמ' 5, וראו סעיף 3 להצעת החוק בתזכיר.

189 **שם**, בעמ' 6.

190 **שם**, בעמ' 7.

191 סעיף 18 להצעת החוק בתזכיר.

192 ראו מבקר המדינה, דו"ח בנושא ועדת הבחירות המרכזית – דוח שנתי 66ג (2016) בעמ' 1820 ואילך.

איומי סייבר,[193] גיבוש תמונת מצב לאומית והתמודדות בזמן אמת עם אירועי סייבר, "לרבות סיוע לארגון בהכלת האירוע, בהתאוששות ממנו ובתחקורו".[194] לשם מימוש אחריותו של מערך הסייבר הלאומי, הצעת החוק בתזכיר כוללת רשימת סמכויות, לרבות סמכויות שטעונות בקשת צווים מבית המשפט.

לפיכך, וכמפורט בפרק ההמלצות להלן, אף שבתזכיר אין התייחסות מפורשת לתהליך הבחירות או לוועדת הבחירות כגוף, נראה כי מערך הסייבר הלאומי מתאים, מעצם תפיסתו כגורם בעל האחריות הכוללת להגנת הסייבר בתחום האזרחי, לשמש כגורם העיקרי להגנתו של תהליך הבחירות בישראל. כאמור לעיל, כבר כיום מתקיימים קשרי עבודה עם ועדת הבחירות המרכזית, אבל קשר זה כאמור וולונטרי, ואינו מכוח אחריות מחייבת. קביעה פורמלית ומפורשת בדבר אחריותו של מערך הסייבר הלאומי להגנת תהליך הבחירות, כחלק מתזכיר חוק הסייבר, דורשת ביצוע התאמות מיוחדות שנובעות מרגישותו של תהליך הבחירות בכלל וייחודיותה של ועדת הבחירות המרכזית בפרט, וכן קביעה של תחומי הכפיפות וגזרות האחריות בינו ובין הגופים האחרים הרלוונטיים להגנה על תהליך הבחירות בישראל.

3. שירות הביטחון הכללי (השב"כ): אחריות ותפקידים

את שאלת אחריותו ותפקידיו של שירות הביטחון הכללי יש לבחון דרך שתי נקודות מבט: האחת – האחריות להגנה מפני התערבות מדינתית זרה באמצעות התקפה מקוונת על מערכת הבחירות בישראל; והאחרת – חידוד היחס בין העצמאות המוסדית והחוקתית של ועדת הבחירות המרכזית ובין כפיפותו של השב"כ לממשלה בכלל ולראש הממשלה, כגורם הממונה על השב"כ מטעם הממשלה, בפרט.

193 ראו סעיף 17 להצעת החוק בתזכיר חוק הסייבר.

194 שם.

מכאן שאת אחריותו של השב"כ בתחום ההגנה על תהליך הבחירות יש לגזור בסופו של דבר מהשילוב בין ייעודו ותפקידיו ובין הכפיפות המוסדית והשיקולים החוקתיים המיוחדים שיש לקחת בחשבון בתחום ההגנה על הבחירות, כמו שיפורט להלן.

א. תפקידי השב"כ בתחום ההגנה על הבחירות

כאמור בחוק השב"כ, הארגון מופקד על:

> שמירת ביטחון המדינה, סדרי המשטר הדמוקרטי ומוסדותיו, מפני איומי טרור, חבלה, חתרנות, ריגול וחשיפת סודות מדינה, וכן יפעל השירות לשמירה ולקידום של אינטרסים ממלכתיים חיוניים אחרים לביטחון הלאומי של המדינה, והכל כפי שתקבע הממשלה ובכפוף לכל דין.[195]

השב"כ הוא הגוף היחיד שבייעודו נכתב במפורש כי הוא מופקד על הגנת "סדרי המשטר הדמוקרטי ומוסדותיו", וכי אחריותו להגנה זו היא מפני אותם איומים קונקרטיים שנקובים בסעיף. שני איומים בסעיף זה עשויים להיות רלוונטיים לעניין בחינת היקף אחריותו של השב"כ להגן על תהליך הבחירות מפני התקפת סייבר שמקורה בישות זרה: איום ה"חתרנות" ואיום ה"חבלה".

כדי להבין אם התיבה "חתרנות" כוללת גם פגיעה בתהליך הבחירות על ידי מעצמה זרה, יש לפנות להגדרת המושג "חתרנות". הגדרה זו מופיעה בתשובת המדינה שניתנה בחודש פברואר 2014 לעתירה שהגישה האגודה לזכויות האזרח.[196] בהתאם לתגובת המדינה, ההגדרה המעודכנת של המונח "חתרנות" כמו שהעביר השב"כ למשרד המשפטים, היא:

> פעילות אף בלתי אלימה שיש בה היבטים חשאיים, הנובעת

195 סעיף 7(א) לחוק שירות הביטחון הכללי, התשס"ב–2002 (להלן: חוק השב"כ).

196 בג"ץ 5277/13 **האגודה לזכויות האזרח בישראל נ' שרות הביטחון הכללי ואח'** (2017) (להלן: בג"ץ 5277/13) – את תשובת המדינה ניתן לראות באתר האגודה לזכויות האזרח (https://tinyurl.com/law-527713).

> ממניעים אידיאולוגיים או מאינטרסים של גורמים זרים, אשר מטרתה או תוצאתה המסתברת היא עבירה על החוק או סיכון ביטחון המדינה, או פגיעה בסדרי המשטר הדמוקרטי או מוסדותיו או פגיעה באינטרסים ממלכתיים חיוניים אחרים לביטחון הלאומי של המדינה אותם קבעה הממשלה בהתאם לחוק השב"כ.[197]

מהגדרה זו עולה כי פעילות שנוקטים גורמים זרים נגד סדרי המשטר הדמוקרטי או מוסדותיו, ודאי אם כרוכה בה הפרת החוק, נכללת בהגדרת ה"חתרנות" שעל סיכולה מופקד השב"כ.

באותו האופן נראה כי פעולת היזק למערכת הבחירות עשויה להיכלל בתיבה של "חבלה" בסדרי המשטר הדמוקרטי או במוסדותיו, שהיא כאמור חלופה נוספת במסגרת ייעודו של השב"כ בהתאם לחוק.

ההגנה על סדרי המשטר הדמוקרטי ומוסדותיו נכללת לא רק בייעודו של השב"כ, אלא הוחלה במפורש כחלק מתפקידיו הקונקרטיים של הארגון הנקובים בחוק השב"כ, שכן תפקיד מרכזי של השב"כ מוגדר כ"סיכול ומניעה" של פעילות בלתי חוקית שנועדה לפגוע בעניין זה.[198]

כדי לממש את תפקידו זה הוקנו לשב"כ סמכויות נרחבות, הן בחוק השב"כ והן בחוקים אחרים, בין היתר סמכויות לקבל ולאסוף מידע,[199] להעביר מידע לגופים אחרים,[200] להקים מאגר נתוני תקשורת ולבצע פעולות במאגר זה לשם מימוש

197 סעיף 31 לתגובה המקדמית של המדינה מפברואר 2014 בבג"ץ 5277/13.

198 סעיף 7(ב)(1) לחוק השב"כ.

199 סעיף 8(א)(1) לחוק השב"כ.

200 סעיף 8(א)(2) לחוק השב"כ.

תפקידיו[201] וכן לבצע פעולות בתוכנם של טקסטים בהתאם לסמכויותיו בתחום החיפוש למטרות מודיעין[202] ובהתאם לחוק האזנת סתר.[203]

עולה מכך שבמסגרת תפקידו למנוע ולסכל חתרנות, נכלל גם התפקיד לסכל ולמנוע פגיעה מטעם מעצמה זרה בסדרי המשטר הדמוקרטי ומוסדותיו, כשתהליך הבחירות הוא חלק מרכזי באותם "סדרי המשטר הדמוקרטי". לשם כך עומדים לרשות השב"כ כלים וסמכויות רבי עוצמה למימוש אחריותו זו, לרבות בדרך של שיתוף גופים אחרים במידע שברשותו. מובן כי אין כל מניעה שבדין כי שיתוף מידע כאמור יתקיים גם עם ועדת הבחירות המרכזית.

תפקיד נוסף מתפקידיו של השב"כ שעשוי להיות רלוונטי לעניין זה הוא לקיים "מחקר מודיעין ומתן ייעוץ והערכת מצב לממשלה ולגופים אחרים שקבעה הממשלה".[204] מאחר שסיכול ומניעה של התערבות זרה בבחירות נכללות בתפקידי השב"כ, עניין זה גורר אחריו גם חובה לקיים מחקר מודיעין בנושא, וכנגזרת מכך לתת – על בסיס מחקר מודיעין זה – "ייעוץ והערכת מצב" לממשלה ולגופים אחרים שהיא תקבע.

מכאן שהשב"כ מוסמך, ובמידה רבה אף נדרש, לייעץ ולתת הערכת מצב בראש ובראשונה לממשלה. נראה שיש טעם לקבוע כי ייעוץ והערכת מצב כאמור יינתנו גם לגופים רלוונטיים אחרים כמו ועדת הבחירות המרכזית, מערך הסייבר הלאומי ובמקרים מתאימים – לגופים נוספים בהתאם למנגנון שיש להשלימו בהחלטת ממשלה מפורשת.

ב. שיקולים לעניין מימוש תפקידי השב"כ בתחום ההגנה על הבחירות

כדי להבין מהם הפרמטרים למימוש תפקידי השב"כ בתחום ההגנה על הבחירות יש להבין כי לעצמאות המוסדית של ועדת הבחירות המרכזית, שבראשה עומד

201 סעיף 11 לחוק השב"כ.

202 סעיף 10 לחוק השב"כ.

203 בהתאם לפרק ב לחוק האזנת סתר, התשל"ט–1979.

204 סעיף 7(ב)(5) לחוק השב"כ.

שופט של בית המשפט העליון, יש חשיבות חוקתית. מעצמאות חוקתית זו נובע כי לוועדה סמכות עקרונית לטפל באיומים על מערכת הבחירות, לרבות איומי סייבר, ומכך נגזרת גם סמכותה להיוועץ עם כל גורם רלוונטי שתמצא לנכון, אבל אין להכפיפה בשום מקרה להנחיות של רשויות הביטחון, אלא להפך. העיקרון שיש לקבוע הוא כי כאשר מדובר בהגנה על מערכת הבחירות, פעולות גופי הביטחון צריכות להיות כפופות להנחיותיו של יושב ראש ועדת הבחירות המרכזית.

עיקרון נוסף שמכתיב את אופן המימוש של תפקידי השב"כ הוא הימנעות עקרונית מפיקוחו על הבחירות ועל ביטוי פוליטי בפרט. כוחו של השב"כ בממלכתיותו ובהימנעותו מלהיכנס לתחום הפוליטי. על הזהירות המיוחדת שעל גוף כמו השב"כ לנקוט אפשר ללמוד ממילות החוק: "השירות יפעל באורח ממלכתי; לא תוטל על השירות משימה לשם קידום אינטרסים מפלגתיים־פוליטיים."[205] מזהירות מיוחדת זו נובע כי בכל הנוגע לתחום הבחירות יש להגדיר את סמכויות השב"כ באופן צר ודווקני כדי שלא לפגוע בחופש הביטוי, בפרטיות ובשוויון. קושי נוסף נובע מהיותו של ראש השב"כ כפוף לראש הממשלה – שהוא שחקן פוליטי – ומהיחס בין כפיפות זו לכפיפות המוצעת ליושב ראש ועדת הבחירות בענייני הבחירות בתקופת הבחירות.

לסיכום נראה כי מצד אחד לשב"כ אחריות ישירה ומפורשת למנוע ולסכל פגיעה בתהליך הבחירות בישראל כשזו נובעת מאיומים הנכללים בייעודו – לענייננו רלוונטיים איומי החתרנות והחבלה. נראה כי כשמדובר בהתערבות של מדינה זרה בתהליך הבחירות בישראל במטרה לקדם אינטרסים של מדינה זרה, עניין זה נכלל במובהק בתפקידי השב"כ. מנגד, אופן מימוש תפקידיו חייב לקחת בחשבון את הרגישות הייחודית הנובעת מהרצון להימנע מפיקוח כלשהו של השב"כ על ביטוי פוליטי בחברה דמוקרטית, וכן מיחסי הכפיפות המיוחדים שמקורם בסוברניות החוקתית של ועדת הבחירות המרכזית מכאן, ומכפיפותו של השב"כ לממשלה ומטעם הממשלה – לראש הממשלה – מכאן.

205 סעיף 4(ג) לחוק השב"כ.

4.
משטרת ישראל: אחריות ותפקידים

המשטרה היא הגוף העיקרי לאכיפת החוק בישראל. פקודת המשטרה קובעת כי תפקידה לעסוק "במניעת עבירות ובגילוין, בתפיסת עבריינים ובתביעתם לדין, בשמירתם הבטוחה של אסירים, ובקיום הסדר הציבורי ובטחון הנפש והרכוש".[206] מכוח פקודת המשטרה נכתבה הוראת המשטרה שכותרתה: "משטרת ישראל – ייעוד, תפקידים, סמכויות ומבנה",[207] שם נקבע כי בין היתר כי המשטרה אחראית לחשוף עבירות ולמנוע את עשייתן; לחקור עבירות שחקירתן לא נמסרה בדין לרשות חוקרת אחרת; לגלות עבריינים ולהביאם לדין; וכן לסייע לרשויות אכיפת חוק אחרות במלאכתן על פי הקבוע בחוק או על פי מדיניות שקבע המפכ"ל.[208]

פגיעה בתהליך הבחירות עשויה לכלול עבירות פליליות רבות, שפזורות בדברי חקיקה שונים, כשהעיקריים בהם הם חוק הבחירות לכנסת, חוק המחשבים וחוק העונשין, כמו שיפורט להלן.

סעיפי העבירה מ**חוק הבחירות לכנסת** הרלוונטיים לפגיעה בבחירות באמצעות התקפת סייבר עשויים להיות בעיקר זיוף פנקס בוחרים או רשימת בוחרים;[209] הפרעת הבחירות[210] ובין היתר גם הפרעה למהלך הסדיר של הבחירות;[211] הצבעה שלא כחוק,[212] שבהתאם לחוק עלולה להיות גם שימוש של אדם באמצעי זיהוי או

206 סעיף 3 לפקודת המשטרה [נוסח חדש], התשל"א–1971.

207 הוראת משטרת ישראל מספר 02.01.01 מיום 3.4.2012.

208 **שם.**

209 סעיף 117 לחוק הבחירות לכנסת.

210 סעיף 119 לחוק הבחירות לכנסת.

211 סעיף 119(א)(1) לחוק הבחירות לכנסת.

212 סעיף 124 לחוק הבחירות לכנסת.

בפנקס זיהוי שאינם שלו, או שנעשה בהם רישום או שינוי כלשהם שלא כדין;[213] או הצבעה יותר מפעם אחת, אם באותה קלפי ואם בקלפיות שונות.[214]

סעיפי עבירה רלוונטיים מ**חוק המחשבים** עשויים להיות שיבוש או הפרעה למחשב או לחומר מחשב[215] לרבות הפרעה לשימוש במחשב,[216] מחיקה או שינוי בחומר מחשב;[217] העברת מידע כוזב למחשב[218] או העברת תוכנה שתוצאת השימוש בה תהיה מידע או פלט כוזבים, כלומר שיש בהם כדי להטעות.[219] עוד קובע חוק המחשבים שחדירה לחומר מחשב שלא כדין – כלומר חדירה באמצעות התקשרות או התחברות עם מחשב, לרבות חדירה למחשב כדי לעבור עבירה אחרת[220] – היא עבירה.[221] כאשר החדירה למחשב מאפשרת קליטת תשדורת או התקשרות בין מחשבים בזמן אמת – זו עשויה להיחשב האזנת סתר אסורה.[222] עוד עבירות לפי חוק המחשבים הן פעולות אסורות בתוכנה שמכוונות לשבש את פעולת המחשב או להפריע לשימוש בו; למחוק חומר מחשב, לשנותו או לשבשו בכל דרך אחרת; או ביצוע פעולות תוכנה שתוצאתן היא מידע כוזב או פלט כוזב; או חדירה לחומר מחשב הנמצא במחשב, שתוצאתן האזנת סתר או פגיעה בפרטיות; וכן החדרה למחשב של התקנים העשויים לבצע אחד מהעניינים המפורטים לעיל.[223]

213 סעיף 124(א)(1) לחוק הבחירות לכנסת.

214 סעיף 124(א)(2) לחוק הבחירות לכנסת.

215 סעיף 2 לחוק המחשבים, התשנ"ה–1995.

216 סעיף 2(1) לחוק המחשבים.

217 סעיף 2(2) לחוק המחשבים.

218 סעיף 3(א)(1) לחוק המחשבים.

219 סעיף 3(א)(2) לחוק המחשבים.

220 סעיף 5 לחוק המחשבים.

221 סעיף 4 לחוק המחשבים.

222 סעיף 2 לחוק האזנת סתר.

223 סעיף 6 לחוק המחשבים.

גם סעיפים רלוונטיים מחוק העונשין עשויים להיות רלוונטיים להתקפת סייבר, לרבות עבירה של הפרעה לבחירות,[224] וכן עבירה של היזק בזדון – הקובע כעבירה הרס של נכס או פגיעה בו במזיד[225] או עבירות מכוח חוק הגנת הפרטיות.[226]

מכאן ועל בסיס אחריותה הכוללת של המשטרה למניעת עבירות, לחשיפתן ולהבאת העבריינים לדין, נראה כי למשטרה יש תפקיד הן במניעת התרחשותן של העבירות הכרוכות בפגיעה בבחירות באמצעות התקפת סייבר, הן בחשיפתן והן בהבאת העבריינים לדין. לשם כך עליה לגבש נוהלי עבודה מתאימים ולקיים שיתוף פעולה הדוק ומתמשך עם הגורמים האחרים המופקדים על הגנת מערכת הבחירות מפני התקפות סייבר שמקורן במדינה זרה.

מכיוון שאת עיקר פעולתה של מערכת האכיפה יש לכוון למניעת פגיעה בתהליך הבחירות, תפקידה של המשטרה לחקור, לאתר חשודים ולהעמידם לדין – עם כל חשיבותו – הוא מאמץ משני למאמץ העיקרי -סיכול הפגיעה ומזעור השפעותיה.

5. המטה לביטחון לאומי (המל"ל): אחריות ותפקידים

המטה לביטחון לאומי הוא גוף המטה העיקרי של הממשלה וראש הממשלה לענייני החוץ והביטחון של מדינת ישראל,[227] אשר מופעל ומונחה על ידי ראש הממשלה. תפקידיו של המל"ל שעשויים להיות רלוונטיים לעניין התקפת סייבר מטעם מדינה זרה הם בין היתר לרכז את עבודת המטה של הממשלה, של ועדת השרים לענייני ביטחון לאומי וכן של כל ועדת שרים אחרת בענייני חוץ

224 סעיף 197 לחוק העונשין, התשל"ז-1977.

225 סעיף 452 לחוק העונשין.

226 חוק הגנת הפרטיות, התשמ"א-1981.

227 סעיף 1 לחוק המטה לביטחון לאומי, התשס"ח-2008.

וביטחון,[228] וכן לבצע כל תפקיד מטה אחר בענייני החוץ והביטחון ובתחום אחר שקבע ראש הממשלה.[229] לשם מימוש תפקידו, הוסמך המל"ל לזמן לדיונים את נציגי גופי הביטחון שראש הממשלה ממונה עליהם, את משטרת ישראל ואת משרדי הממשלה שנוגעים לנושא שעליו מתקיימת עבודת המטה.[230]

בעקבות הניסיון שנצבר במדינות אחרות בשנים האחרונות, נראה כי איום התקפות סייבר על מערכת הבחירות בישראל הוא איום מוחשי, שעלול לפגוע בחוסנה הלאומי של מדינת ישראל, ולכן כלול בתפקידיו של המטה לביטחון לאומי שכן זהו הגורם העיקרי האחראי על גיבוש הצעת מדיניות כוללת, לרבות הצעת חלופות, והבאתה לממשלה או לוועדות השרים הרלוונטיות.

6. קצין הכנסת: אחריות ותפקידים

קצין הכנסת הוא הגורם האחראי על הגנת הכנסת מכוח חוק משכן הכנסת, רחבתו ומשמר הכנסת.[231] על פי האמור בחוק, קצין הכנסת מופקד על "שמירת הביטחון ועל קיום הסדר במשכן הכנסת, וברחבה, על אבטחת מידע מסווג של הכנסת או מידע מסווג המצוי ברשותה, ובקשר לכל אלה".[232] לשם מימוש תפקידיו ניתנו בידי קצין הכנסת סמכויות שונות, לרבות סמכויות מפקד מחוז במשטרה.[233] במילים אחרות, קצין הכנסת הוא רשות סטטוטורית מכוח חוק

228 סעיף 2(א)(1) לחוק המטה לביטחון לאומי.

229 סעיף 2(א)(11) לחוק המטה לביטחון לאומי.

230 סעיף 2(ב) לחוק המטה לביטחון לאומי.

231 סעיף 8 לחוק משכן הכנסת, רחבתו ומשמר הכנסת, התשכ"ח-1968 (להלן: **חוק משכן הכנסת**).

232 סעיף 8(ב) לחוק משכן הכנסת.

233 סעיף 8(ג) לחוק משכן הכנסת.

משכן הכנסת ורחבתו, ולפיכך הוא סוברני בהחלטותיו. יש לציין כי מבחינה ארגונית יחידת המחשב של הכנסת כפופה למנכ"ל הכנסת.

מעקרון הפרדת הרשויות, מעצמאות הכנסת ומעמד קצין הכנסת נובע כי כיום היחסים בין קצין הכנסת למערך הסייבר או לשב"כ מתקיימים על בסיס וולונטרי. מאחר שהכנסת היא יעד לתקיפות מחשב – הן תקיפות מחשב של הכנסת כגוף והן של חברי הכנסת כיחידים -שיתוף הפעולה עם הרשויות האחרות (השב"כ, מערך הסייבר) מתקיימים שלא מכוח הנחיה, אלא בהתאם להחלטתו של קצין הכנסת. גם מערכת היחסים בין קצין הכנסת לוועדת הבחירות המרכזית מבוססת על שיתוף פעולה וולונטרי, שכן קצין הכנסת רואה בוועדת הבחירות גוף עצמאי ונפרד מהכנסת, אף שמבחינה פיזית ועדת הבחירות יושבת במשכן הכנסת.[234]

מאחר שחברי הכנסת והעוזרים הפרלמנטרים משתמשים במשאבי מחשב שמספקת להם הכנסת, ומאחר שחברי כנסת ועוזרים פרלמנטרים עשויים להחזיק במידע שפגיעה בו – אם בדרך של שיבוש ואם בדרך של גנבה והפצה – עלולה להשפיע על טוהר הבחירות לכנסת, נראה כי אחריות קצין הכנסת לשמירה על הביטחון במשכן הכנסת וברחבה ועל אבטחת מידע מסווג של הכנסת מטילה עליו חובות בנוגע לאבטחת חברי הכנסת ועוזריהם הפרלמנטרים גם מפני התקפות סייבר.

נוסף על חברי הכנסת והעוזרים הפרלמנטרים, ובהתאם לאמור בחוק, מתוך משכן הכנסת פועלת גם ועדת הבחירות המרכזית,[235] שמשתמשת גם היא בשירותי המחשוב שנותנת הכנסת. מכאן שפעילותה של ועדת הבחירות מצויה בתוך "משכן הכנסת ורחבתו" שעל הגנתו מופקד קצין הכנסת, ויש לבחון גם את השאלה אם אחריות זו כוללת גם פעולות מניעה והגנה מפני תקיפת סייבר על ועדת הבחירות המרכזית.

מימוש אחריותו של קצין הכנסת בהיבטים של אבטחת המידע שברשות חברי הכנסת מתבטאת באבטחת חשבונות הדואר האלקטרוני שלהם והתקנת מערכות אבטחה במחשבים האישיים ובטלפונים הניידים שמספקת להם הכנסת.

234 שיחה עם אופיר כהן – ממונה אבטחת מידע בקצין הכנסת.

235 סעיף 29א לחוק משכן הכנסת.

העוזרים הפרלמנטרים משתמשים לעיתים בחשבונות הדואר האלקטרוני של הח"כים ולעיתים בחשבון הדואר האלקטרוני שנפתח בשבילם במערכות הכנסת ובאחריות האבטחה של קצין הכנסת.

יש לציין כי כאשר חבר הכנסת פותח חשבון דוא"ל אישי, אתר אינטרנט או למשל חשבון פייסבוק – קצין הכנסת אינו רואה עצמו אחראי על אבטחתם של עניינים אלה, ומכאן שיש להבהיר את שאלת האחריות על אבטחתם.

נראה כי יש לחדד מהי אחריותו של קצין הכנסת לאבטחת חברי הכנסת והעוזרים הפרלמנטרים מפני התקפות סייבר ולקבוע את כללי הפעולה הנגזרים מאחריותו זו, לרבות כללי העדכון והדיווח של קצין הכנסת בהיבטים אלה לוועדת הבחירות המרכזית, למפלגות ולמערך הסייבר הלאומי.

7. משרד הפנים: אחריות ותפקידים

המשרד הממשלתי העיקרי שוועדת הבחירות המרכזית פועלת עמו (בלי שמתקיימים בין הגופים יחסי כפיפות) הוא משרד הפנים. שר הפנים הוא השר הממונה על ביצוע חוק הבחירות לכנסת,[236] והוא שמוסמך להתקין תקנות בעניין ביצוע החוק, בהסכמתה של ועדת הבחירות המרכזית או בהמלצתה.[237]

כאמור, מאגר המידע העיקרי המשמש את ועדת הבחירות המרכזית הוא פנקס הבוחרים, שהכנתו באחריות משרד הפנים.[238] הפנקס כולל את פרטיו האישיים של כל אדם שביום שליפת הפנקס היה אזרח ישראלי הרשום במרשם האוכלוסין כתושב ויום הולדתו ה־18 חל לא יאוחר מיום הבחירות. רשימת הבוחרים בפנקס

236 סעיף 150 לחוק הבחירות לכנסת.

237 סעיף 145 לחוק הבחירות לכנסת.

238 סעיף 26(ד) לחוק הבחירות לכנסת.

מחולקת בהתאם לאזורי הקלפי שאליהם משויך כל בוחר המתגורר באזור שלה.[239] משרד הפנים אחראי לתקן את הרשימה בהתאם להחלטות בפניות ובבקשות לתיקון שהפנו אליו אדם או ועדת הבחירות המרכזית, וכן אחראי לתקן את הפנקס בהתאם להחלטה של בית משפט מוסמך.[240] על שר הפנים למסור את פנקס הבוחרים שהכין לוועדת הבחירות המרכזית במועדים הקבועים בחוק.[241]

מכאן שהאחריות הכוללת על הכנת פנקס הבוחרים, תקינותו, מהימנותו, לרבות הגנה עליו מפני היזק או זיוף שמקורו בהתקפת סייבר מוטלת על משרד הפנים בהתאם להנחיות מערך הסייבר הלאומי.

8. הרשות להגנת הפרטיות ורשם מאגרי המידע: אחריות ותפקידים

הרשות להגנת הפרטיות במשרד המשפטים היא הגוף המאסדר את הכללים הנוגעים למאגרי מידע, המפקח על ביצוע כללים אלה והאוכף את החקיקה הרלוונטית, וזאת בהתאם לחוק הגנת הפרטיות.[242] לפיכך הרשות מופקדת על הגנת המידע האישי במאגרי מידע דיגיטליים ומפעילה רגולציה שבצידה אכיפה מינהלית ופלילית על כלל הגופים המחזיקים או מעבדים מידע אישי דיגיטלי בהתאם לחוק הבחירות לכנסת,[243] פנקס הבוחרים הוא מאגר מידע שיש לו הגנה מיוחדת, שכן חוק הבחירות קובע הוראה עונשית־פלילית על מי שמשתמש

239 סעיף 26(ג) לחוק הבחירות לכנסת.

240 סעיפים 53 ו־53א לחוק הבחירות לכנסת.

241 סעיף 71 לחוק הבחירות לכנסת.

242 משרד המשפטים, "שומרים על הפרטיות שלך במרחב הדיגיטלי" (סרטון), **אתר הרשות להגנת הפרטיות**.

243 סעיף 39(ה) לחוק הבחירות לכנסת.

במידע מפנקס הבוחרים שלא כדין.[244] כדי שהרשות תוכל לממש את תפקידה, נקבע בחוק כי על שר הפנים להודיע לרשם מאגרי המידע ברשות להגנת הפרטיות לאילו מפלגות או סיעות נמסר מידע מפנקס הבוחרים.

אחריותה של הרשות, אפוא, היא להבטיח, באמצעות קביעת רגולציה מתאימה, כי פנקס הבוחרים יזכה להגנה מיוחדת, וכי הוצאת הפנקס לגופים מורשים תלווה בהוראות מתאימות ובפיקוח על מימושן.

9. יחידת הסייבר בפרקליטות המדינה: אחריות ותפקידים

יחידת הסייבר בפרקליטות המדינה היא יחידה ארצית שעוסקת בריכוז ההתמודדות המשפטית עם פשיעת סייבר.[245] היחידה היא גורם המטה המוסמך בפרקליטות המדינה לתחום הסייבר לרבות בתחום האכיפה המינהלית[246] ועבירות מחשב. היא מנהלת בעצמה תיקים פליליים בנושא, והיא המנחה המקצועית לפרקליטים ולגורמי האכיפה בתחומים אלה. עוד מתפקידה של היחידה לבצע את המהלכים המשפטיים הנדרשים למימוש האכיפה, לרבות

244 סעיף 118א לחוק הבחירות לכנסת.

245 באתר האינטרנט של הפרקליטות "פשיעת סייבר" כוללת את סוגי העבירות האלה:

עבירות נגד מחשב ונגד מידע – חדירה לחומר מחשב, הפצת וירוסים, סוסים טרויאניים ותולעים, הפרעה לפעולת מחשב (כגון בדרך של התקפות DdoS), גניבת מידע ממוחשב (מידע אישי, מידע בעל ערך כלכלי, מידע בעל חשיבות לביטחון הלאומי) ועוד.

עבירות קלאסיות שהועתקו במלואן למרחב הממוחשב – המדובר בעבירות מגוונות (מרמה, זיוף, הימורים, פרסומי תועבה פדופיליים, הטרדה מינית ועוד)".

ראו אתר פרקליטות המדינה/ מחוזות ומחלקות/ יחידת סייבר/ אודות. אוחזר ביום 21.12.2018.

246 חיים וישמונסקי "אכיפה אלטרנטיבית של עברות ביטוי במרחב הסייבר" **משפט צדק? ההליך הפלילי בישראל – כשלים ואתגרים** 691 (אלון הראל עורך, 2017).

"פעילות להסרת תכנים פוגעניים, סינונם מתוצאות החיפוש, הרחקת משתמשי אינטרנט המבצעים פעילות אסורה, ואמצעי התגוננות, מניעה וסיכול במרחב הסייבר בכלים משפטיים".[247]

מכאן שיחידת הסייבר בפרקליטות המדינה היא הגורם המבצע בפועל או כמנחה מקצועית הן בתחום התביעה והן בתחום האכיפה המינהלית. ככזאת יש לה תפקיד חשוב במימוש החלטותיה של ועדת הבחירות המרכזית הנוגעות לאכיפה מינהלית במרחב המקוון, וכן בליווי חקירות שמבצעים גורמי הביטחון או משטרת ישראל בנושאים אלה.

10.
לסיכום: התחומים החשופים לתקיפות סייבר והאחריות להגנה עליהם – תמונת מצב

כאמור לעיל, את ההגנה על מערכת הבחירות בישראל יש לגזור מהאחריות הכללית בעיקר של ועדת הבחירות המרכזית, מערך הסייבר הלאומי, השב"כ ומשטרת ישראל – כל אחד בתחום תפקידיו. כיום אחריות זו מתבצעת בעיקר בהתאם לשיקול דעתם של גופים אלה. מהאמור לעיל עולה כי יש לקבוע אחריות מוסדית ופורמלית של כלל הגופים הרלוונטיים להגנה על תהליך הבחירות וזאת בתחומים שסומנו ככאלה, שתקיפתם באמצעות המרחב המקוון עלולה לפגוע בתהליך הבחירות ובאמון הציבור בתוצאותיו, כדלקמן:

א. הגנה על ביצוע הבחירות

(1) הגנה על פנקס הבוחרים – באחריות משרד הפנים (בהנחיית מערך הסייבר הלאומי).

247 שם.

(2) הגנה על שלבי ביצוע הבחירות – האחריות אינה מוגדרת מפורשות. בפועל באחריות ועדת הבחירות המרכזית, המקיימת יחסי הנחיה וולונטריים עם מערך הסייבר הלאומי.

ב. הגנה על מפלגות ועל שחקנים פוליטיים

(1) הגנה על מפלגות. האחריות אינה מוגדרת, לא בהיבט של תכולת ההגנה, לא בהיקפה ולא מיהו הגורם האחראי עליה. בפועל ההגנה באחריות מנכ"לי המפלגות.

(2) הגנה על חברי הכנסת ועל עוזריהם הפרלמנטרים. האחריות אינה מוגדרת מפורשות. נראה כי קיימת אחריות מסוימת לקצין הכנסת, בעיקר בכל הנוגע לשימושם של חברי הכנסת והעוזרים הפרלמנטרים במשאבי הכנסת (כתובות דוא"ל וחומרה) בסיוע וולונטרי של מערך הסייבר הלאומי. לא ברור מי אחראי על אבטחתם של חברי הכנסת והעוזרים הפרלמנטרים בכל הנוגע לשימוש במחשב, בחשבונות דואר אלקטרוני ובאתרים אישיים שאינם מונפקים על ידי הכנסת.

(3) הגנה על אישים פוליטיים שאינם חברי כנסת. לא ברור מי נמנה עם אישים אלה (ראשי מפלגות שאינם חברי כנסת? מועמדים לכנסת?) ומי אחראי על הגנתם מפני תקיפות סייבר.

ג. סיכול מניפולציה ברשתות חברתיות ובאתרי חדשות שמטרתה להשפיע על הבחירות

לא ברור מהן ההגדרות האופרטיביות לקביעה מהי מניפולציה שמכוונת להשפיע על הבחירות, מי אחראי לאיתור פעילות להשפעה כזאת של ישות זרה, ומהם הכלים המותרים לאיתורה. מניתוח האמור לעיל נראה כי האחריות לאיתור תקיפה כזאת היא של מערך הסייבר הלאומי, וכשמאותרת תקיפה של ישות זרה, נראה כי האחריות העקרונית לסיכול פעילות כזאת היא של שירות הביטחון הכללי. בנוסף, לא ברור מהם כללי הכפיפות וכללי הדיווח, בעיקר בנוגע ליחס בין האחריות החוקתית של ועדת הבחירות המרכזית על טוהר הבחירות במובנו הרחב, ובין כפיפותם של ארגוני הביטחון למרות הממשלה. בנוסף, לא ברור מהם עקרונות התיאום והתיחום בין גורמי הביטחון והאכיפה השונים בתחום רגיש זה, מהם העקרונות ליידוע הציבור ועוד.

פרק 1

המלצות מדיניות

מטרתן של המלצות המדיניות שיפורטו להלן לחזק ולשפר את ההגנה על תהליך הבחירות במובנו הרחב מפני התקפות במרחב המקוון על ידי ישויות זרות, בין היתר במטרה לשמור על אמון הציבור בתוצאות הבחירות. המלצות אלה נגזרות מהאיומים שנחשפו בשנים האחרונות בזירה הבינלאומית ורלוונטיים גם לתהליך הבחירות בישראל על מגוון היבטיו. ההמלצות יתייחסו למגוון ממדים – משפטיים, מוסדיים ומושגיים – בשלוש זירות התקיפה שתוארו: הגנה של תהליך ביצוע הבחירות; הגנה של השחקנים הפוליטיים; והגנה מפני תקיפות ברשתות החברתיות.

מובן כי ניטור הרשת לשם הגנה על בחירות חופשיות ודמוקרטיות אינו חף מסיכונים. הסכנה הגדולה היא שמעקב אחר פעילות הבוחרים, התעמולה ופעולתם של פעילים פוליטיים עלולה ליצור אפקט מצנן על חופש הביטוי וכן לפגוע בפרטיות ובשוויון בבחירות. אינטרסים אלה מצויים בליבת ההליך הדמוקרטי. הקושי העיקרי הוא כי אי־אפשר להניח שניתן יהיה לזהות איומים אסטרטגיים מחוץ לישראל בלי להיזקק למידה כלשהי של ניטור ומעקב אחר פעילות שמתבצעת בתוכה. מכאן שלנוכח הרגישות המיוחדת של תהליך הבחירות – בייחוד בחברה שסועה ומפולגת כמו החברה הישראלית – תנאי מוקדם לכל רגולציה או חקיקה בנושא הוא הערכה של השפעת הרגולציה על חופש הביטוי, על הגנת הפרטיות ועל זכויות אזרח אחרות.

המלצות אלה אינן תחליף לפעולות הנדרשות ממקבלי ההחלטות ומעצבי המדיניות לחיזוק החוסן הציבורי, להרגעת השיח הציבורי ולטיפול בהתנהלות אלימה וקיצונית בעודה באיבה. מבחינה מעשית, כדי לתת מענה מערכתי לאיומים שנסקרו לעיל, יש להסדיר מפורשות את אחריותה הכוללת של ועדת הבחירות המרכזית להגנה על מערכת הבחירות (במובן הרחב של המושג) ולשמירה על אמון הציבור בתוצאות הבחירות ותקינות ההליך הדמוקרטי.

ההמלצות שלהלן יתייחסו בעיקרן לפעולות של רשויות הממשל שיש בהן כדי לשפר את המוכנות המערכתית, את חלוקת האחריות בין הגופים, את מנגנוני התיאום הנדרשים ואת הסמכויות למימושם. ההמלצות לא יתייחסו לפעולות תקיפה־שכנגד של יעדים שיזוהו ככאלה שמהם עלולה לצאת מתקפת סייבר

שמטרתה התערבות במערכת בחירות בישראל.[248] זאת ועוד, ייתכן שיש מקום לעודד מעורבות של הסקטור הפרטי והמגזר השלישי (עמותות) הן בפיתוח יכולות, והן במנגנון שיתמרץ פיתוחים לאיתור תקיפות מבוססות־מדינה ברשתות החברתיות, ליצירת מנגנוני בדיקה של עובדות לאיתור מהיר של דיסאינפורמציה מאורגנת, ועוד.

1.
המלצות לעניין הגנה על תהליך הבחירות מפני התקפות סייבר שמקורן בישות זרה

א. כללי

ועדת הבחירות המרכזית ויושב ראש הוועדה הם הגורמים שלהם האחריות הכוללת להגנה על תהליך הבחירות, כאשר את מהלכי הניטור והסיכול בפועל יבצעו הגופים והרשויות האמונים על כך, בהנחייתה של ועדת הבחירות המרכזית. קביעה זו מאזנת בין הצורך לתת מענה מערכתי ובין הצורך להרחיק את השרים, שהם שחקנים פוליטיים, מטיפול בנושא. לפיכך ליד יושב ראש ועדת הבחירות יש להקים ועדה מייעצת, שתכלול נציגים מכלל גופי הביטחון הרלוונטיים לרבות השב"כ, המשטרה, המוסד, מל"ל וצה"ל. הוועדה תהיה אחראית לגבש את תמונת האיומים העדכנית (שכן קצב השינויים הטכנולוגיים מחייב עדכון מתמיד) ואת תפיסת המענה לאיומים אלה. יושב ראש ועדת הבחירות יהא ריבוני להחליט אילו מהמלצות הוועדה המייעצת ייושמו.

248 לפי פרסומים בתקשורת האמריקאית (אוקטובר 2018) הפנטגון, באמצעות פיקוד הסייבר, הוציא לפועל תקיפות סייבר נגד אנשים שזוהו ככאלה שעלולים לפגוע, באמצעות התקפות סייבר, במערכת בחירות־האמצע בארצות הברית. ראו Luis Martinez, Pentagon Launches Cyber Operation to Prevent Russian Meddling in Midterm Elections, ABC News (October 25, 2018)

גופי הביצוע העיקריים יהיו מערך הסייבר הלאומי והשב"כ: מערך הסייבר הלאומי הוא גוף אזרחי במהותו, שייעודו העיקרי להגן על המדינה ועל מערכותיה מפני התקפות סייבר. לכן יש לו תפקיד חשוב בקביעת התקנים המקצועיים ובהנחיה של כלל הגופים הרלוונטיים לנושא.

השב"כ הוא הגוף המתאים ביותר – מבחינת כלל היכולות, לרבות תהליכי העבודה וטכנולוגיה – לאיתור וסיכול מעורבות של מדינה זרה במערכת הדמוקרטית בישראל. יש מקום להקצות לו משאבים ייעודיים כך שיוכל להתאים את המענים לשינויים ולאיומים בנושא חשוב זה. כמו כן, וכחלק מהמענה המערכתי, יש מקום לחדד את תפקידו ברוח חוק השב"כ, המגדיר את אחריותו של הארגון בהגנה על הדמוקרטיה בישראל. החידוד נדרש כדי לשמור על האיזון בין הצורך להגן על הדמוקרטיה ובין הצורך להרחיק את הארגון מכל הקשר פוליטי, בייחוד בשל העובדה שהעומד בראשו כפוף ישירות לראש הממשלה – שחקן פוליטי בהגדרה. יש מקום לתקן את חוק השב"כ בנושא של התערבות במערכת הדמוקרטית של ישראל בכלל ובכל הקשור למערכת הבחירות בפרט, כך שבנושאים אלו ידווח ראש השב"כ גם – ובמקרים מסוימים רק – ליושב ראש ועדת הבחירות. יושב ראש ועדת הבחירות יהיה מוסמך (בהתייעצות עם הוועדה המייעצת) לפרסם את המידע לציבור – כולו או חלקו – מתוך מתן משקל ראוי לעקרון השקיפות, שהוא אחד המגינים החשובים על הדמוקרטיה.

כללי דיווח אלה יש להחיל גם על הגופים האחרים לאכיפת החוק. כך למשל אם הוגשה למשטרת ישראל תלונה על התערבות זרה במערכת הבחירות, יהא עליה לדווח על כך ליושב ראש ועדת הבחירות.

את כלל המערכות המשמשות למימוש של תהליך הבחירות (כמו שפורטו לעיל) יש להגדיר "תשתית קריטית", כמו שנעשה במדינות אחרות בעולם. החלה כזאת תגדיר באופן מלא את מכלול ההגנה עליה, לרבות היבטים של הגנת סייבר והגנה פיזית, וכן את נוהלי ההתאמה הביטחונית של עובדי מערכת הבחירות. לעניין זה יש לכלול את כלל המערכות הפריפריאליות למערכת הבחירות המרכזית (אם עדיין אינן כלולות), כגון המערכת במשרד הפנים האחראית על הכנת פנקס הבוחרים. הגדרת תהליך הבחירות כ"תשתית קריטית" תיבדל מאופן ההגדרה של שאר התשתיות הקריטיות בכך שבעניין תהליך הבחירות הגופים המנחים כגון השב"כ ומערך הסייבר הלאומי יספקו את ההמלצות, אבל ועדת הבחירות המרכזית היא שתבחר אילו מההמלצות לממש.

לצורך יישום ההחלטה יש להקצות תקציב ייעודי שיתווסף לתקציב ועדת הבחירות המרכזית ויאפשר לה לבצע את אותן ההמלצות שיוחלט לממש. ועדת הבחירות תדווח למליאת הוועדה (שחברים בה נציגים מכל סיעות הבית) אילו המלצות הוחלט לאמץ ומהו סטטוס היישום שלהן.

מעת לעת נשמעים קולות הקוראים לוועדת הבחירות המרכזית לאמץ מערכת הצבעה אלקטרונית כדי להחיש את קצב ספירות הקולות בתום תהליך ההצבעה.[249] אנו קוראים לוועדת הבחירות לדבוק בשיטה הקיימת – הצבעה בפתקי נייר וספירה ידנית על ידי ועדות הקלפי. אף ששיטה זו אינה חסינה מפני רמאות (ראו פסילת קולות החיילים בבחירות המקומיות 2018 בתל אביב), בהשוואה למערכת אלקטרונית קשה יותר לרמות בה בהיקף גדול. זאת ועוד, מאחר שפתקי ההצבעה המקוריים נשמרים, כשמתעורר חשד להתערבות, אפשר לחזור ולספור את פתקי ההצבעה באופן שקוף ומעורר אמון יותר משאפשרי במערכת מחשבית.

ב. ההמלצות

המלצה 1: מוצע לקבוע שהאחריות הכוללת על הגנת תהליך הבחירות מפני התערבות של ישות זרה תוטל על ועדת הבחירות המרכזית.

מוצע לקבוע בחוק, עקרונית ותפיסתית, כי האחריות הכוללת להגנה על מערכת הבחירות מפני התקפות סייבר שמקורן בישויות מחוץ למדינה תוטל על ועדת הבחירות המרכזית, וכנגזרת מכך לקבוע את האחריות והסמכויות של יושב ראש הוועדה. עוד מוצע לקבוע מפורשות כי העצמאות החוקתית והמוסדית של ועדת הבחירות המרכזית תישמר גם בתחום זה, כך שהוועדה תקבל המלצות ממערך הסייבר ומגורמי הביטחון האחרים ותקבע אילו מהן ימומשו. מוצע לקבוע כי את פעולות אבטחת המידע הדרושות להגנה על תהליך הבחירות מפני תקיפות סייבר, לרבות שכירת מומחים מקצועיים מתאימים, תתקצב ועדת הבחירות המרכזית, ואוצר המדינה הוא שיישא במימון.

249 כך למשל בשנת 2009 הגיש ח"כ מאיר שטרית הצעת חוק פרטית שמטרתה לאפשר הצבעה ממוחשבת בבחירות לרשויות המקומיות, בעקבות תוכנית חלוץ (פיילוט) שהתקיים בכמה קלפיות בבחירות 2007. ראו הצעת חוק הרשויות המקומיות (בחירות) (תיקון – בחירות ממוחשבות), התשס"ט–2009. הצעת החוק לא קודמה מאז.

הסבר: כמפורט לעיל, תהליך ההכנה והמימוש של הבחירות מתחיל בהכנת ספר הבוחרים ומסתיים בסיום העתירות והעררים לאחר פרסום תוצאות הבחירות. לכל אורך התהליך פזורות אפשרויות לתקיפה מקוונת, בהסתברות הצלחה ובתוחלת נזק משתנה. הגורם המופקד על הבחירות בישראל הוא ועדת הבחירות המרכזית, ולפיכך יש לקבוע בחוק הבחירות לכנסת כי האחריות להגנת התהליך תוטל עליה ולהקנות לה את האמצעים למימוש אחריותה.

המלצה 2: מוצע לכונן ועדה מייעצת קבועה ליושב ראש ועדת הבחירות המרכזית לעניין הגנת תהליך הבחירות מפני התקפות סייבר שמקורן בישות מדינתית זרה.

לנוכח החשיבות הגדולה שבהגנה על תהליך הבחירות, ומאחר שהאחריות המעשית מתחלקת בין כמה גופים, הצורך בפעולה מתואמת שתתבצע בקצב ובמועד שיאפשרו סיכול או מזעור של הפגיעה בתהליך הבחירות, מצדיק את כינונה של ועדה מייעצת קבועה ליושב ראש ועדת הבחירות המרכזית. מוצע לקבוע כי בראשות הוועדה יעמוד ראש מערך הסייבר הלאומי, וחבריה יהיו נציג בכיר של השב"כ, נציג בכיר של המוסד, נציג משטרה בכיר וקצין הכנסת.

תפקידי הוועדה המייעצת יהיו:

(**1**) לרכז ולשתף את המידע בין הגופים בנוגע להתקפות סייבר נגד תהליך הבחירות;
(**2**) להמליץ ליושב ראש ועדת הבחירות המרכזית על דרכי הפעולה לאיתור של תקיפה כזאת, הגורם האחראי לה והדרך לסיכולה או למזעור פגיעתה;
(**3**) להמליץ ליושב ראש ועדת הבחירות המרכזית המלצות לעניין פרסום המידע לציבור, כולו או חלקו, לרבות לעניין המועד לכך.

המלצה 3: מוצע להכריז על תהליך הבחירות בתור "תשתית לאומית קריטית".

מוצע לתקן את חוק הבחירות לכנסת ולקבוע בו הוראות שעיקרן הכרזה על תהליך הבחירות לכנסת כתשתית קריטית; להגדיר את העניינים הנכללים ב"תהליך הבחירות לכנסת" מתוך הבחנה בין הגנה על התשתיות (מידע ומערכות) מפני פריצה, דליפה ושינוי, ובין הגנה מפני מניפולציה מכוונת להשפעה על הבחירות; לקבוע את אחריותו של מערך הסייבר הלאומי להציע את הפעולות הנדרשות לאבטחת מערכות המחשב שהן חלק מביצוע הבחירות, ואת אחריותו של השב"כ להציע את סוגי המשרות שיסווגו בסיווג ביטחוני;

לקבוע את סמכותו של יושב ראש ועדת הבחירות המרכזית לאשר או לדחות המלצות אלה; ואת אחריותו של מנכ"ל ועדת הבחירות המרכזית למימושן.

הסבר: תהליך הבחירות בישראל הוא תשתית קריטית לתפקודה התקין של המדינה, שכן אמונו של הציבור בתהליך בחירתם של מוסדות השלטון של המדינה ואמונתו שהתהליך התבצע באופן מהימן חיוניים מאין כמותם למשטר הדמוקרטי. בארצות הברית הוכרז תהליך הבחירות "תשתית קריטית" בשנת 2017, על המשתמע מכך. להכרה זו משמעות פורמלית והצהרתית בדבר חשיבות הבחירות, וגם משמעות מעשית – בספקה מסגרת פעולה מוכרת שגוררת אחריה אחריות לביצוע שורות של פעולות הגנה ותקצובן.[250]

החוק להסדרת הביטחון בגופים ציבוריים הוא האכסניה הרשמית להכרזה על גופים ועל מערכות מחשביות כתשתיות חיוניות,[251] ומכאן להחיל עליהם אסדרה שתבטיח שייקבעו תקני אבטחה באמצעות מערכות ההנחיה שנקבעו לכך, לרבות סמכויות בקרה ופיקוח על מימושן, והכול כדי להבטיח שהמערכות החיוניות לתפקודה התקין של המדינה יהיו מוגנות כדבעי. בשל מבנהו הכללי ומטעמים של הפרדת רשויות, נראה כי החוק להסדרת הביטחון – המחייב להכפיף את תהליך הבחירות לסמכויות ההנחיה של גופי הביטחון – אינו מתאים לשמש אכסניה מתאימה לקביעת תהליך ההכרזה ונגזרותיו, לרבות הסמכויות והביצוע של קביעת הסטנדרטים לאבטחת תהליך הבחירות כתשתית קריטית. ולכן נדרש תיקון חוק הבחירות

המלצה 4: מוצע לקבוע שהמטה לביטחון לאומי (מל"ל) יגבש תפיסה כוללת להגנה על מערכת הבחירות בישראל מפני התערבות זרה.

הסבר: מכיוון שמדובר בעניין מערכתי בעל חשיבות לאומית עליונה, שמתעדכן מעת לעת עם שינויי הטכנולוגיה והתפתחות האיומים, מוצע להטיל על המל"ל לגבש תפיסה לאומית כוללת ולהביאה לאישור הגורמים המוסמכים – הממשלה או הקבינט.

250 מייד לאחר ההכרזה, במרץ 2017, הקציב הקונגרס 380 מיליון דולר לשדרוג האבטחה של מערכות הבחירות.

251 חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.

2. המלצות לעניין ההגנה על שחקנים פוליטיים מפני התקפות סייבר שמקורן בישות זרה

א. כללי

מפלגות משתמשות במערכות מחשב לצרכים מגוונים – החל בבחירות מקדימות, עבור במערכות לתכנון הקמפיין וכלה בניהול הלוגיסטיקה של יום הבחירות. ברם מערכות אלה חשופות לאיומי תקיפה. מוצע כי מטה הסייבר הלאומי יחויב להנחות את המפלגות באשר לאופן ההגנה המומלץ, אבל המפלגות ישמרו על עצמאותן בהחלטה אילו מההמלצות לממש. לצורך המימוש מוצע כי מימון המפלגות יוגדל בתקציב "צבוע", שבו יוכלו המפלגות להשתמש רק לצורך הגנה מפני איומי סייבר. מטה הסייבר יוכל גם להמליץ על נותני שירותים תחום ההגנה מפני איומים, והמפלגות יוכלו לבחור בעצמן בספק זה או אחר לפי שיקול דעתן.

ב. ההמלצות

המלצה 5: מוצע להסדיר את אחריות ההגנה על המפלגות הפוליטיות מפני התקפות סייבר ואת אופן מימושה.

מומלץ לקבוע כי האחריות להגנתה של מפלגה פוליטית מפני התקפות סייבר תוטל על מנכ"לי המפלגות; מוצע לקבוע כי ועדת הבחירות המרכזית היא שתעביר למפלגות את כללי האבטחה מפני התקפות סייבר על בסיס ההמלצות שיעביר לוועדה מערך הסייבר הלאומי; מוצע לקבוע כי בחוק מימון המפלגות ייכלל סכום "צבוע" שיוכל לשמש אך ורק לאבטחת המידע של המפלגה בהתאם לסטנדרטים שתקבע ועדת הבחירות המרכזית.

הסבר: מפלגות פוליטיות הן השחקניות העיקריות בזירה הפוליטית. מקצתן מקיימות הליכי בחירה פנימיים (פריימריז) מבוססי מחשב, ויש ברשותן מידע שהעתקתו או שיבושו עלולים לגרום נזק אלקטורלי למפלגה. בתחום זה אין כל רגולציה מחייבת, וכל מפלגה פועלת כטוב בעיניה.

לנוכח הסיכון הרב הקיים בתקיפת סייבר מצד ישות זרה, ופוטנציאל הנזק לתהליך הבחירות הגלום בכך, הצורך למנוע התקפות כאלה, לאתר אותן ולסכל אותן הוא אינטרס ציבורי חשוב. לכן יש להטיל אחריות פורמלית, לקבוע את הגורם האחראי לקביעת תקן האבטחה הנדרש ו"לצבוע" את המקור התקציבי למימונה.

כדי לשמור על עצמאותן של המפלגות כך שלא יוכפפו להנחיות של רשות ממשלתית שמטבע הדברים כפופה לשחקנים פוליטיים, מוצע כי מערך הסייבר יחויב לתת את השירות, אבל המפלגות ישמרו על עצמאותן בהחלטה אילו המלצות לממש.

המלצה 6: מוצע להטיל את האחריות להגנה על חברי כנסת ועל עוזריהם הפרלמנטרים על קצין הכנסת.

מוצע לקבוע מפורשות כי אבטחת המידע שברשות חברי הכנסת ועוזריהם הפרלמנטרים, על כלל שימושיהם בחשבון הדואר האלקטרוני של הכנסת, בציוד מחשב ובטלפונים סלולריים שמספקת הכנסת, לרבות אבטחתם מפני תקיפת סייבר, היא באחריותו של קצין הכנסת. לנוכח החשיבות הציבורית הרבה שיש להגנת סייבר על התהליך הדמוקרטי בכלל ועל תהליך הבחירות בפרט, מוצע שלא להותיר את כללי האבטחה ליחסים וולונטריים בין מערך הסייבר ובין קצין הכנסת, אלא לקבוע דגם מחייב יותר. לפיכך מומלץ לקבוע מפורשות כי את כללי האבטחה שיחולו על קצין הכנסת לעניין אבטחת המידע של חברי הכנסת ועוזריהם הפרלמנטרים תקבע ועדת הבחירות המרכזית בהתאם להמלצות של מערך הסייבר הלאומי, ואלה יעודכנו מזמן לזמן. עוד מוצע לקבוע בכללים אלה כי על קצין הכנסת לדווח למערך הסייבר הלאומי ולוועדת הבחירות המרכזית על כל חשד לתקיפת סייבר של חברי כנסת או מי מעוזריהם הפרלמנטרים.

הסבר: חברי הכנסת משתמשים בחשבונות דואר אלקטרוני שמספקת להם הכנסת, מתוך שרתי מחשב המצויים בכנסת. בנוסף, חברי הכנסת מקבלים לשימושם מאת הכנסת טלפונים ניידים ומחשבים אישיים ונייחים. גם עוזריהם הפרלמנטרים של חברי הכנסת רשאים לקבל חשבון דואר אלקטרוני מהכנסת ובפועל חלקם עושים כך. האחריות על חשבון הדוא"ל של הכנסת ועל ציוד המחשב שמספקת הכנסת צריך להיות באחריות האבטחה של קצין הכנסת ומכאן ההמלצה.

המלצה 7: מוצע להטיל את האחריות להגנה על שימושי מחשב של חברי כנסת שאינם באחריות קצין הכנסת, וכן את ההגנה מפני תקיפות סייבר על אישים פוליטים שאינם חברי כנסת על מנכ"לי המפלגות.

מוצע לקבוע כי מנכ"לי המפלגות יחויבו לדאוג להגנה של חשבונות הדואר האלקטרוני, האתרים האישיים והחשבונות ברשתות החברתיות של חברי כנסת ואישים פוליטיים שאינם חברי כנסת, וכן של מועמדים לכנסת מטעם הרשימה שאינם חברי כנסת. כללי אבטחת המידע יועברו אליהם מוועדת הבחירות המרכזית בהתאם להמלצות שיתקבלו ממערך הסייבר הלאומי.

הסבר: אישים פוליטיים מרכזיים שאינם חברי כנסת (למשל יושב ראש מפלגה פוליטית שנבחר לתפקיד בטרם התקיימו בחירות לכנסת) עשויים להיות יעד להתקפת סייבר שמקורה בישות זרה, ופגיעתה של תקיפה כזאת עלולה להשפיע על תהליך הבחירות ועל תוצאותיהן. בהיעדר גורם אחר, נראה כי האחריות לאבטחת אישים אלה מפני התקפות סייבר צריכה להיות מוטלת על המפלגה שאליה הם שייכים.

המלצה 8: מוצע לקבוע, בהמלצה או בהוראת חוק מחייבת, שהבחירות המקדימות במפלגות יתבצעו בעזרת פתקי הצבעה ולא במערכת ממוחשבת.

הסבר: מאחר שלדעת מומחי אבטחה בכירים[252] כיום אי־אפשר ליצור מערכת הצבעה ממוחשבת שתהיה מאובטחת דיה כדי למנוע בוודאות פריצה של מעצמה זרה, מוצע להמשיך ולבחור באמצעות פתקי הצבעה, כמו שאכן נעשה במערכת הבחירות הכלליות ובמערכת הבחירות המקומיות. כאמור לעיל, גם הצבעה בפתקי נייר אפשר לזייף, אבל בהשוואה למערכת ממוחשבת קשה יותר לעשות זאת בהיקפים גדולים, וקל יחסית לחזור ולספור את הפתקים הנשמרים בוועדת הבחירות גם שנים לאחר ביצוע הבחירות. היגיון זה חל גם בבחירות המקדימות, שכיום מתבססות על הצבעה ממוחשבת.

252 מומחה אבטחת המידע ברוס שנייר מתנגד נחרצות להצבעה במכונות הצבעה, בדואר אלקטרוני או באפליקציה: "This is crazy (and dangerous). West Virginia is allowing people to vote via a smart-phone app. Even crazier, the app uses blockchain – presumably because they have no idea what the security issues with voting actually are." Bruce

3.
המלצות לעניין התמודדות עם מבצעי השפעה מבוססי סייבר שמקורם בישות זרה ברשתות חברתיות ובאתרי חדשות

א. כללי

כפי שעולה מהניסיון במדינות אחרות, במטרה להשפיע על הבחירות התערבו מדינות זרות ברשתות החברתיות ובשאר אמצעי התקשורת המקוונים במגוון שיטות ואמצעים. מוצע להקים גוף ייעודי – יחידת ניטור – שיעסוק בניטור תכנים באינטרנט. גוף זה לא יעקוב אחר גופים או יחידים שמזוהים כישראלים וכן לא יעסוק ב"צנזורה של תכנים ברשת". מטרתו תהיה לזהות ניסיון של מדינה או גופים מחוץ לישראל להשפיע על הדמוקרטיה באופן חשאי, שאין בו ייחוס לישות העומדת מאחוריו ולכן אינו שיח פוליטי לגיטימי. השפעה כזאת יכולה להיעשות באמצעות דיסאינפורמציה, חדשות כזב (פייק ניוז), מסרים מפלגים ומשסים, הסתה לאלימות, שימוש בחשבונות פיקטיביים (בוטים וטרולים) ועוד. מוצע כי גוף זה יהיה חלק ממערך הסייבר הלאומי, אבל על פעולתו יפקחו יושב ראש ועדת הבחירות המרכזית או מועצה ציבורית שבראשה יעמוד שופט בדימוס.

לכשיעלה חשש כי מדינה או גוף זר מנסים להשפיע על הבחירות בישראל באמצעות התערבות ברשתות החברתיות ובאמצעים אחרים מבוססי רשת, ידווח ראש יחידת הניטור ליושב ראש ועדת הבחירות המרכזית, והוא יהיה

Schneier, *West Virginia Using Internet Voting*, Schneier on Security (19.10.2018); וכן Schneier, *American Elections*, **לעיל** ה"ש 28. גם מומחים אחרים סבורים כך, למשל: "There is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats" Securing the Vote: Protecting American Democracy 94–95 (National Academies of Sciences, Engineering, and Medicine, 2018) doi: https://doi.org/10.17226/25120

סוברני להחליט כיצד לפעול: החל באי־נקיטת כל פעולה וכלה בסיכול הפעילות העוינת לרבות הבאת העניין לידיעת הציבור. בהתאם להחלטתו של יושב ראש ועדת הבחירות המרכזית יופעלו גופי הביטחון הנוגעים לעניין.

גוף הניטור יהיה אחראי לשיתופי הפעולה עם השחקניות הגדולות ברשת כגון פייסבוק וגוגל במטרה לפעול באופן האפקטיבי ביותר.

ב. ההמלצות

המלצה 9: מוצע לקבוע כי הגורם האחראי להגנה מפני פעולות השפעה מבוססות סייבר ברשתות חברתיות ובאתרי חדשות יהא מערך הסייבר הלאומי.

מוצע לקבוע כי מערך הסייבר הלאומי יופקד על ניטור הרשתות החברתיות באינטרנט לשם איתור פעולות סייבר של ישויות זרות שמטרתן להשפיע על תהליך הבחירות בישראל. גוף זה לא יעקוב אחר גופים או יחידים המזוהים כישראלים, וכן לא יעסוק ב"צנזורה של תכנים ברשת". מטרתו תהיה לזהות ניסיון של מדינה או גופים מחוץ לישראל להשפיע על הדמוקרטיה, ולצורך כך ייקבעו תבחינים לזיהוי תכנים שהם חלק ממתקפה של ישות זרה על מערכת הבחירות בישראל. מוצע לקבוע כי לכשיתגלה מהלך כזה, הוא ידווח ליושב ראש ועדת הבחירות המרכזית ולשב"כ. מוצע כי הסדרים לעניין האחריות לטיפול בתקיפה כאמור ולסיכול שלה ייקבעו בין מערך הסייבר הלאומי לשב"כ בהנחייתו של יושב ראש ועדת הבחירות המרכזית.

לנוכח רגישות העיסוק בנושא, מוצע לשקול הקמתה של יחידה ייעודית לעניין זה שתהיה חלק ממערך הסייבר הלאומי, בדומה למנגנון שהוקם בבריטניה,[253] ועליה יפקחו יושב ראש ועדת הבחירות המרכזית או גוף שבראשו שופט בדימוס. גוף הפיקוח יבטיח שמשימות היחידה יוגבלו לזיהוי שימוש ברשתות החברתיות שמטרתו להשפיע על תהליך הבחירות בישראל למען אינטרסים זרים.

253 בבריטניה הוקמה יחידה הלאומית לאבטחת תקשורת (National Security Communications Unit) שמשימתה להילחם בדיסאינפורמציה שמכוונים שחקנים מדינתיים או אחרים, והיא מדווחת ישירות לקבינט. ראו Peter Walker, *New National Security Unit Set Up to Tackle Fake News in UK*, The Guardian (January 23, 2018)

הסבר: ניטור רשתות חברתיות הוא עניין שמגלם בתוכו בעייתיות מובנית בהיבטים רבים שנובעים מעצם הפיקוח, מההגבלות על חופש הביטוי העלולות לנבוע מפיקוח זה ועוד. בנוסף, את הרשתות החברתיות מפעילים תאגידי ענק טכנולוגיים כמו פייסבוק וטוויטר, ולכן פעולה יעילה מחייבת מידה של שיתוף פעולה עימם. על פי המידע באתר הרשמי של פייסבוק, כיום, בעקבות הביקורת הציבורית שספגה לאחרונה, החברה אכן פועלת בנושא.[254] כך למשל בבחירות האמצע בארצות הברית בנובמבר 2018 הפעילה החברה "חדר מלחמה" להתמודדות עם קמפיינים של פייק ניוז ברשת החברתית.[255]

לנוכח אופייה האזרחי של הרשת והצורך לשתף פעולה עם התאגידים המפעילים את הרשתות החברתיות ואת אתרי חדשות, נראה כי נכון שמערך הסייבר הלאומי, כגורם שאמון על פעולה בשוק האזרחי, יהיה הגורם האחראי לפעולות הניטור ברשת ולהסדרי שיתוף הפעולה עם ענקיות התקשורת. לנוכח רגישות העניין מוצע לקבוע כי ייקבעו כללי דיווח לעניין זה בין מערך הסייבר הלאומי לבין יושב ראש ועדת הבחירות המרכזית והשב"כ, המופקד על סיכול פעילות חתרנית שמפעילה ישות זרה. מוצע כי אופן הטיפול ייקבע בהסדרים בין הגופים ובכפוף להנחיותיו של יושב ראש ועדת הבחירות המרכזית.

המלצה 10: מוצע לקבוע כי הפרסום ברבים של חשיפת מבצע השפעה שארגנה ישות זרה יהיה בסמכותו של יושב ראש ועדת הבחירות המרכזית ובכפוף להחלטתו.

מאחר שרכיב אפשרי ואפקטיבי בסיכול עשוי להיות עצם החשיפה של המבצע ופרסומו לציבור, ולנוכח הרגישות הגדולה שיש בסוג כזה של פעולה, מוצע לקבוע כי על פרסום כאמור יוסמך להחליט אך ורק יושב ראש ועדת הבחירות המרכזית.

254 Facebook, *Working to Stop Misinformation and False News* (Facebook for Media, April 7, 2017)

255 Nathaniel Gleicher (Head of Cybersecurity Policy), *Election Update* (Facebooks Newsroom, November 5, 2018)

המלצה 11: מוצע להגיע להסדרי שיתוף פעולה בינלאומיים לאיתור מקור תקיפה שזוהתה.

מוצע להטיל על מערך הסייבר הלאומי ועל השב"כ להגיע להסדרי שיתוף פעולה עם מדינות רלוונטיות כדי שבמקרה הצורך אפשר יהיה לזהות מהר ובבירור את מקור התקיפה. מאפיין מרכזי בעבודתו של גוף הניטור יהיה הייחוס (Attribution), כלומר ייחוס פעולות ברשת לאדם או לארגון מזוהה. בהקשר זה חשוב לציין את המלצת הוועדה שבחנה את חוק דרכי תעמולה בראשותה של הנשיאה ביניש,[256] שממנה נגזרת כעת הצעת חקיקה, המחייבת ייחוס של כל מסר, אתר, קמפיין וכדומה, כך שהציבור יוכל לדעת מי עומד מאחוריו. גוף הניטור יתחקה במיוחד אחר מסרים שאינם ניתנים לייחוס במטרה לזהות את מקורם. לעניין זה יש לחזק כאמור את שיתופי הפעולה עם מפעילי הפלטפורמות הגדולות ברשת. עוד יש לחתור לגיבוש אמנה בין־מדינתית שבה יוגדרו הכללים לסיוע בין מדינות בכל הנוגע לייחוס פרסומים אנונימיים ברשת שאינם ניתנים לייחוס ביכולותיה של כל מדינה בנפרד. כך למשל ניתן יהיה לאבחן כי כמות חריגה של מסרים בעברית מגיעה ממדינה במזרח אירופה ולהחשידה כהתערבות לא לגיטימית של מדינה זרה במערכת הדמוקרטית של ישראל.

הסבר: גם כשמתגלה תקיפה, הייחוס – כלומר קביעה מהירה, ברורה ומשכנעת בנוגע למקור התקיפה – הוא אתגר לא פשוט, שכן התיווך המקוון מאפשר לתוקף לטשטש את זהותו, והניסיון מלמד שתוקפים מתוחכמים אכן פועלים כך. לנוכח חומרת האיום מוצע להטיל מפורשות על מערך הסייבר הלאומי ועל השב"כ לקיים מארג שיתוף פעולה עם עמיתים רלוונטיים כדי לאפשר ייחוס מהיר וברור של תקיפת סייבר שמקורה בישות זרה.

המלצה 12: מוצע לקבוע אמנה שבה יתחייבו המפלגות להימנע מהפעלת חשבונות וירטואליים (בוטים וטרולים) כחלק מקמפיין פוליטי, ישירות או בעקיפין.

כדי לצמצם את האפשרות לשימוש בחשבונות פיקטיביים ולהגביר את השקיפות, מוצע לקבוע אמנה בין־מפלגתית שלפיה כל המפלגות מתחייבות להימנע מהפעלת חשבונות וירטואליים, ישירות או באמצעות אחרים.

256 הוועדה הציבורית לבחינת חוק הבחירות (דרכי תעמולה) התשי"ט–1959, **דין וחשבון** (ירושלים 2017).

הסבר: זה מהלך משלים שנועד להגדיל את המחויבות ההדדית, את חוסר הלגיטימיות שבשימוש בכלים כאלה בקמפיין פוליטי, ואת ה"קנס" הציבורי אם יתברר כי מפלגה או שלוחיה נקטו דרך זו.

המלצה 13: מוצע לקבוע איסור פלילי מפורש על קנוניה חשאית (collusion) בין אזרח או תושב ישראל ובין ישות זרה במטרה להשפיע על הבחירות.

הסבר: כדי להרתיע גורם ישראלי שעשוי להיות בעל עניין בהטיית הבחירות מקנוניה חשאית עם ישות מדינתית זרה – אף שייתכן ששיתוף פעולה כזה עשוי להקים עבירה גם לפי הדין הקיים – מוצע לקבוע זאת כאיסור פלילי מפורש במטרה לחדד את האיסור ולקבוע לו ענישה פלילית ראויה. את האיסור יש לנסח באופן מצומצם וחד, כך שלא יפגע בפעילות ראויה שאין כוונה להגבילה.

המלצה 14: מוצע לעודד הקמה של מערכת אזרחית רחבה לניטור ולבדיקה של עובדות.

הסבר: חלק ממנגנון החיסון הציבורי נגד הטיה מכוונת עשוי להתבצע על ידי מערכת של בדיקת עובדות שתוכל לאתר במהירות חדשות כזב (פייק ניוז), כלומר מידע שקרי, מניפולטיבי ומאורגן. נראה שרצוי שמערכת כזאת תפעל במגזר השלישי, במסגרת עמותות ומכוני מחקר.

המלצה 15: מוצע לבחון את האפשרות לחקוק חוק האוסר על שימוש במידע אישי לשם מיקרו-טרגטינג פוליטי, או לכל הפחות לחייב שקיפות ברורה של הנמענים שמדובר בהודעה פוליטית.

מוצע לשקול את האפשרות למנוע שימוש במידע אישי לשם מיקרו־טרגטינג פוליטי. ואת ההשלכות של איסור זה, על ידי ייסוד מנגנוני סנקציה על חברות פרסום שיימצא שהן מפרות את הנורמה. לכל הפחות יש לחייב חברות שפועלות להעברת מסרים פוליטיים ממוקדים להודיע מפורשות לנמעני המסרים כי מדובר במסרים מטעם גוף פוליטי, כך שהנמען יוכל להעריך את משקל הדברים בפריזמה זו.

הסבר: איסוף נרחב של מידע על פרטים, המאפשר לבנות פרופיל אישי ממוקד ולהתאים מסרים בהתאם לפרופיל ולהעדפות הקונקרטיות של הנמען, עלול

לשמש פלטפורמה בעלת עוצמה ממשית להשפעה על עמדות החשופים לה. בשונה מעולם הפרסום, המשתמש ביכולות של איסוף ופרסום ממוקד לפי העדפות הצרכנים, כשמדובר בזירה הפוליטית יש ערך ציבורי מיוחד להגבלה של השפעה פוליטית מסוג זה, או לכל הפחות יש לחייב הודעה מפורשת לנמען שמדובר במסר מטעם גוף פוליטי.

נספח

תיקוני חקיקה מוצעים

1. תיקון חוק הבחירות לכנסת [נוסח משולב], התשכ"ט-1969

(1) לחוק הבחירות לכנסת יוסף פרק שיקבע כי תהליך הבחירות הוא "תשתית לאומית חיונית".

עיקרי הפרק יהיו כדלקמן:

(**א**) הגדרת "תהליך הבחירות לכנסת";

(**ב**) קביעה כי תהליך הבחירות לכנסת הוא תשתית לאומית חיונית;

(**ג**) מינוי ועדה ביטחונית מייעצת קבועה ליו"ר ועדת הבחירות לכנסת וקביעה של הרכבה ותפקידיה;

(**ד**) הסמכת יושב ראש ועדת הבחירות לתת הנחיות לכל רשות מרשויות המדינה כדי להבטיח את טוהר תהליך הבחירות, ובכלל זה להנחות את ה"קצינים המוסמכים", כהגדרתם בחוק להסדרת הביטחון בגופים ציבוריים, לממש את סמכותם הקבועה בחוק להסדרת הביטחון, לשם הבטחת טוהר הבחירות לכנסת;

(**ה**) הסמכת יושב ראש ועדת הבחירות לכנסת להורות למשטרה לפתוח בחקירה, במקרה של חשד לפגיעה בתקינות תהליך הבחירות לכנסת;

(**ו**) קביעת הוראות עונשין למי שלא מקיים את הנחיותיו של יושב ראש ועדת הבחירות לכנסת בעניין זה;

(**ז**) קביעת הוראות לעניין מימון הגנת תהליך הבחירות מפני התקפות סייבר;

תיקונים עקיפים (אם יידרשו) – בחוק הסייבר, בחוק השב"כ, בפקודת המשטרה ובחוק להסדרת הביטחון בגופים ציבוריים.

(2) ליושב ראש ועדת הבחירות תוקנה הסמכות להנחות את מנכ"לי המפלגות לעניין כללי אבטחת המידע של מפלגה, לרבות לעניין קיום בחירות מקדימות ואבטחת מידע של יושב ראש המפלגה ושל מועדי המפלגה לבחירות לכנסת, בהתאם להמלצות שיעביר אליו מערך הסייבר הלאומי.

(3) ליושב ראש ועדת הבחירות המרכזית תוקנה הסמכות ליתן הנחיות לקצין הכנסת לעניין אופן אבטחת המידע של חברי הכנסת ושל עוזריהם הפרלמנטרים בהתאם להמלצות שיעביר אליו מערך הסייבר הלאומי.

(**4**) בהתאם להמלצת הוועדה הציבורית לבחינת חוק הבחירות (דרכי תעמולה), התשי"ט-1959, ולפיה יש להחיל "את הוראות החוק המהותיות גם באינטרנט וברשתות החברתיות", **ייקבע מפורשות כי חובת הייחוס חלה גם על מי שמפרסם תעמולת בחירות באינטרנט וברשתות החברתיות.**

2. תיקון חוק העונשין, התשל"ז-1977

תיקבע הוראה מפורשת הקובעת כעבירה פלילית הזמנה או שיתוף פעולה עם ישות זרה (מדינה או ארגון זר שאיננו מדינה) למטרת השפעה על בחירות;

3. תיקון חוק המפלגות, התשנ"ב-1992

ייקבע שמנכ"לי המפלגות הם האחראים לאבטחת המידע של המפלגה, של יושב ראש המפלגה ושל מועמדים לכנסת מפני התקפות סייבר.

4. תיקון חוק משכן הכנסת רחבתו ומשמר הכנסת, התשכ"ח-1968

תיקבע בחוק אחריות קצין הכנסת לאבטחת המידע של חברי הכנסת והעוזרים הפרלמנטריים בהתאם להנחיות יושב ראש ועדת הבחירות המרכזית, וכן כללי דיווח של קצין הכנסת למערך הסייבר הלאומי וליושב ראש ועדת הבחירות המרכזית על כל אירוע בו יש חשש לתקיפת סייבר של חבר כנסת או של עוזר פרלמנטרי.

5. תיקון חוק מימון מפלגות, התשל"ג-1973

בחוק מימון המפלגות יוסף מימון הוצאות אבטחת המידע של מפלגות מפני התקפות סייבר. חישוב המימון והגבלה לפיה מימון הוצאות אבטחת מידע מפני התקפות סיבר יוכל להיות מוצא למטרה זו בלבד.

6. תיקון חוק שירות הביטחון הכללי, התשס"ב-2002

ועדת הבחירות המרכזית תוסף לרשימת הגופים להם ייתן השירות "ייעוץ והערכת מצב";

ועדת הבחירות המרכזית תוסף לרשימת הגופים הזכאים לקבל מידע משירות הביטחון הכללי לצורך מילוי תפקידיה של הוועדה.

7. תיקון תזכיר חוק הסייבר

תיקבע אחריות פורמלית למערך הסייבר הלאומי לעניין הגנה על תהליך הבחירות;

ייקבעו יחסי הכפיפות בין המערך לוועדת הבחירות המרכזית בתחום זה;

ייקבעו עקרונות התיאום וחלוקת האחריות בתחום ההגנה על תהליך הבחירות עם שירות הביטחון הכללי;

המרואיינים

ועדת הבחירות המרכזית: יושב ראש ועדת הבחירות המרכזית – השופט חנן מלצר; היועץ המשפטי של ועדת הבחירות המרכזית – עו"ד דין ליבנה

המטה לביטחון לאומי: המשנה לראש המל"ל – מר איתן בן דוד; המל"ל – מר אבנר שמחוני

מערך הסייבר הלאומי: ראש מערך הסייבר הלאומי – מר יגאל אונא; ראש מכלול עמידות במערך הסייבר הלאומי – מר רפי פרנקו

סגן קצין הכנסת: מר אופיר כהן

מנכ"לי מפלגות פוליטיות: מר ציון סוקי ומר גיל סגל

נשיאת איגוד האינטרנט הישראלי: פרופ' קרין נהון

תודות

אנו מודים מקרב לב לכל המרואיינים שהקדישו מזמנם וחלקו עימנו את ניסיונם ואת מחשבותיהם בנושא. תודה מיוחדת לפרופ' ניבה אלקין־קורן, לפרופ' יובל שני, לד"ר חיים ויסמונסקי, לד"ר דנה בלאנדר ולגב' קרן גליקליך – על הערות והארות מחכימות ומועילות.

Policy Paper 136

DEFENDING ISRAEL'S ELECTIONS FROM CYBER-ATTACK – WHAT SHOULD BE DONE?

Ron Shamir | Eli Bachar

DRAFT

January 2019

Text Editors [Hebrew]: Yehudit Yadlin, Keren Gliklich
Series and Cover Design: Studio Tamar Bar Dayan
Typesetting: Nadav Shtechman Polischuk
Printed by Graphos Print, Jerusalem

ISBN: 978-965-519-248-3

The Israel Democracy Institute
4 Pinsker St., P.O.B. 4702, Jerusalem 9104602
Tel: (972)-2-5300-800; Fax: (972)-2-5300-867
E-mail: orders@idi.org.il
Website: en.idi.org.il

The Federmann Cyber Security Center – Cyber Law Program
The Faculty of Law, The Mount Scopus Campus Jerusalem
Box 80, ZIP Code: 9190501
E-mail: hcsrcl@mail.huji.ac.il
Website: https://csrcl.huji.ac.il

ABSTRACT

This study examines the threats posed by intervention in (or influence of) Israel's Knesset elections—in their broadest sense—by means of cyber-attacks conducted by foreign entities, whether at the state or sub-state level. These threats are very real, as recent years have seen multiple cases of states intervening in elections in other countries using internet-based technology. The study does not look at attempts to influence the electoral process by non-internet means; nor does it cover attempts to influence the elections by Israeli political actors, unless they are acting via a foreign entity, or are being knowingly used by a foreign entity in order to influence the elections by internet-based means.

The goals of the study are to map and identify the main threats to the electoral process and to public trust in the election results, as the public's confidence that the winners and losers are determined by a process that was not falsified or interfered with in any other way is essential for our most basic social foundations. These threats are assessed based on the technological, legal, and institutional environment in which the defense of Israel's elections takes place, and policy recommendations are then offered based on this assessment.

Of the countries that over the last decade have been identified as engaging in operations to exert influence via cyber tools, Russia has been the most prominent—albeit not the sole—example, having attempted to intervene in elections in Ukraine (2014), the United States (2016), France (2017), Germany (2017), and the Netherlands (2017), as well as in referenda in the United Kingdom, the Netherlands, Italy, and Spain (2017). These actions were generally intended to support a particular candidate or weaken others, while at least some had other goals as well: to create social rifts in those countries over substantial issues and thus weaken social unity; to advance strategic goals, such as weakening the NATO pact; to undermine the principle of abiding by international norms; and to damage public trust in the democratic process.

Cyberspace offers a range of means and methods for influencing elections, such as: theft of information from political figures and disseminating it in a way and at a time that will hurt opponents; corrupting information within the election system—ranging from altering the electoral register to altering results—in order to undermine public trust in the results; preventing use of systems by inflicting DDOS (distributed denial of service) attacks at a pre-determined time, and in places that use electronic voting systems, attacking the computerized voting machines; creating and spreading fake news over social networks; hoaxing third parties, such as journalists, by using false identities on the web; and more.

Experience shows that attempts to intervene in elections involve three main types of attack: (a) attacking the execution of the electoral process at any of its stages, whether via forgery or by interference with or denial of service; (b) attacks on political parties and figures using various means, including stealing personal and political information and publicizing it at an advantageous time, interfering with party preparations for the elections, and more; and (c) attacking social networks and news sites as sources of major influence over voters' political positions, using cyber tools.

Cyber-attacks on the electoral process may include the use of technological tools such as bots and big data technology; use of advanced tools for hacking into computer systems; and the use of paid trolls, infiltration of innocent web forums, and more. These tools have been used, for example, in operations aiming to disseminate misleading information to a very large audience; to steal information and selectively publicize it at a time that will have most impact on the elections; in personalized micro-targeting operations; in operations to exert influence by damaging infrastructure; and more. What all these efforts tend to have in common is that the source of the attacks is masked, making it very difficult to determine which state or organization is behind them, and to clearly identify the attacker.

The outcomes of the cyber-attacks on elections in the United States and other Western countries in recent years have shown that no country can remain indifferent to the very real threat of cyber-attacks against its electoral process and against public trust in the election results. Thus, a series of actions are required, in terms of both defense and deterrence, in order to significantly bolster the resilience of democracies and to effectively protect them against such attacks. However, when liberal democracies seek to defend themselves against attacks of this kind, many questions arise regarding democratic principles and concepts, chief among them being how to ensure that activities designed to prevent attacks on the electoral process will not themselves be used to harm such liberal democratic principles as freedom of expression, privacy, and equality.

Cyber-attacks intended to harm Israel's electoral process could be carried out in all the ways in which electoral systems have been attacked in other countries. In addition, Israel is a riven and polarized society with strong internal tensions over many questions: Jewish-Arab relations, religion and society, the future of the occupied territories, and more. Thus, striking at social consensus over the electoral mechanism as the main national expression of democracy and as the source of the government's

legitimacy—and as a way of undermining public trust in the election results—could be particularly deleterious to the social bindings that allow Israel's social disagreements to play out within a functioning society. Because of this, protecting the electoral process in Israel carries special importance.

A review of the institutional structure of the organizations that are responsible for various elements relating to the security of the electoral system—in its broadest sense—against cyber-attacks reveals that this responsibility is divided (as detailed in the study) among several entities, including the Central Elections Committee, the National Cyber Directorate, the Israel Security Agency, the Israel Police, the Knesset Sergeant-at-Arms, the Ministry of the Interior, the Privacy Protection Authority, and the Registrar of Databases and the Cyber Unit in the State Attorney's office.

It appears that the overall responsibility for protecting the elections themselves from cyber-attack lies with the Central Elections Committee, while the preliminary stage (preparing the electoral register) is the responsibility of the Ministry of the Interior. It is not clear who is responsible for protecting political parties, and in practice this is handled by the party directors-general. As regards political figures who might be targets for attack, the Knesset Sergeant-at-Arms is partially responsible for data security for serving members of Knesset and their parliamentary aides, but it is not clear who is responsible for protecting political figures who are not Knesset members from cyber-attack. The issue of influencing elections via manipulation of social media and news websites is the most problematic for defining and setting clear responsibilities, and here the division of responsibility between the National Cyber Directorate and the Israel Security Agency should be properly examined.

The main problem lies in the fact that monitoring the internet in order to protect free and democratic elections is an activity that itself carries noticeable dangers for democracy, as there is a concern that tracking the

activities of voters and of political activists may serve to limit freedom of expression and impinge on privacy and equality in the elections—interests that lie at the heart of the democratic process. Consequently, the precondition for any regulation or legislation on this issue must be an assessment of its impact on freedom of expression, on privacy protections, and on other civil rights, given the particular sensitivity of the electoral process.

Moreover, the extreme sensitivity of the electoral process requires unique rules of subordination and reporting, especially regarding the relation between the constitutional responsibility of the Central Elections Committee for the purity of the elections in their broadest sense, and the fact that the security organizations report directly to the government. It is also necessary to set principles for organizational coordination and boundaries regarding this issue between the security and enforcement agencies themselves, principles for notifying the public, and more.

The following policy recommendations are intended to strengthen and improve the defense of the electoral process in Israel, in its broadest sense, from cyber-attacks by foreign entities, both in order to prevent any undue influence on the election results and to maintain public trust in those results.

The main recommendations are as follows:

(1) The overall responsibility for protecting the elections process from foreign intervention should be given to the Central Elections Committee, with a clear ruling that the constitutional and institutional independence of the Committee will be maintained in this field as well. Consequently, the responsibilities and powers of the chairperson of the Central Elections Committee in this regard should be clearly defined.

(2) A permanent advisory committee should be appointed to advise the chairperson of the Central Elections Committee on protecting the electoral

process from cyber-attacks by foreign state entities. The roles of this advisory committee will include coordinating and sharing information between the various bodies regarding cyber-attacks on the electoral process; recommending to the chairperson methods of identifying such an attack and its source, and means for thwarting it or limiting its harmful effects; and making recommendations to the chairperson on publicizing the fact that an attack has taken place, whether partially or fully, including the timing of such an announcement.

(3) The elections process should be declared a "critical national infrastructure," anchored in the Knesset Elections Law.

(4) The National Security Council (NSC) should formulate an overall approach for the defense of Israel's electoral system from foreign intervention, and submit it for approval by the relevant body—the government or the cabinet.

(5) Regulations should be introduced stating which body has responsibility for protecting political parties from cyber-attacks and how this should be done in practice, and funding should be made available, including via "designated funds" set aside in the parties' election budgets, so that each party can implement the security proposals autonomously.

(6) Responsibility for protecting members of Knesset and their parliamentary aides should lie with the Knesset Sergeant-at-Arms, and rules should be set down for reporting between the various entities involved in protecting the electoral process from any suspicion of cyber-attack against members of Knesset or their parliamentary aides.

(7) The directors-general of political parties should be made responsible for protecting their Knesset members' use of computers that are not under the jurisdiction of the Knesset Sergeant-at-Arms, as well as defending against cyber-attacks on political figures who are not members of Knesset. The directors-general should apply data security

rules that will be issued by the Central Elections Committee, based on recommendations from the National Cyber Directorate.

(8) It should be made a requirement, either via recommendation or by a binding act of legislation, that primary elections within political parties should be held using paper voting slips and not computerized systems.

(9) The National Cyber Directorate (NCD) should be made responsible for defense against any cyber-based attempts to influence elections via social networks and news websites. If any such attempts are identified, they should be reported to the chairperson of the Central Elections Committee and to the Israel Security Agency (ISA). Arrangements for which body is responsible for dealing with these attacks should be agreed between the NCD and the ISA, with the approval of the chairperson of the Central Elections Committee. Due to the sensitivity of this subject, a dedicated unit should be set up within the NCD to handle it, overseen by a body headed by a retired justice. This body will ensure that the unit's activities are restricted to identifying use of social networks to influence elections in Israel to serve foreign interests.

(10) The chairperson of the Central Elections Committee should have the power to decide whether to make public the discovery of an attempt by a foreign entity to influence the elections.

(11) Agreements should be reached for international cooperation to identify the source of any attacks discovered, including attempts to conclude an international treaty.

(12) A covenant should be agreed in which all political parties commit to refraining from operating virtual accounts (bots and trolls) as part of their political campaigns, whether directly or indirectly.

(13) The act of collusion between an Israeli citizen or resident and a foreign entity with the aim of influencing the elections should be made a

criminal offense. This offense should be worded carefully so as to restrict it only to relevant cases, and prevent it from being used against worthy activities that are not the target of this legislation.

(14) The establishment of a broad civil system for fact checking should be encouraged, as part of the public resilience mechanism to defend against targeted misdirection.

(15) The possibility should be explored of passing a law that forbids the use of personal information for political micro-targeting, or at the least, that requires full transparency for those being targeted that the message being presented is from a political source.

Implementing these recommendations, and paying continued institutional attention to technological changes and developments in the field of cyber-attacks, can strengthen Israel's ability to defend itself and also increase public awareness of the issue, which is an essential component of democratic resilience.

בשנים האחרונות זוהו מקרי התערבות לא מעטים מצד מדינות בתהליכי הבחירות של מדינות אחרות באמצעות טכנולוגיה המבוססת על האינטרנט. תחומי הפעולה העיקריים היו תקיפה של תהליך ביצוע הבחירות, תקיפת מפלגות ושחקנים פוליטיים וניסיונות להשפיע על תודעת הבוחרים באמצעות מניפולציות ברשתות החברתיות. פעולות התערבות כאלה נועדות בדרך כלל לתמוך במועמד מסוים או להחליש אחר, אך גם לקדם מטרות אסטרטגיות קונקרטיות של המדינה המתערבת. מקצתן גם מיועדות להחליש בחברה המותקפת את הלכידות החברתית ולפגוע באמון הציבור בתהליך הבחירות, וכנגזרת מזה – לפגוע באמון הציבור בשיטה הדמוקרטית עצמה. סכנת ההשפעה חמורה במיוחד במדינות המתאפיינות בשסעים חברתיים עמוקים, וישראל נמנית בהחלט עם מדינות אלו.

עם זה אין לשכוח שכאשר דמוקרטיה ליברלית, ובכלל זה מדינת ישראל, מבקשת להתגונן מפני התקפות כגון אלו עולות שאלות עקרוניות מהותיות – החשובה שבהן: כיצד להבטיח שפעולות התגוננות מפני התקפות המכוונות לפגוע בתהליך הבחירות הדמוקרטי לא יפגעו, הן עצמן, בערכי יסוד של הדמוקרטיה כמו חופש הביטוי וערכי הפרטיות והשוויון.

ההצעות הנכללות במחקר זה מבקשות לתת ביטוי לאיזונים חיוניים אלו.

רון שמיר הוא יזם, מנכ"ל חברת פונטיקה (העוסקת בתחום ה־Med-Tech) וחוקר במרכז המחקר להגנת הסייבר בפקולטה למשפטים באוניברסיטה העברית בירושלים. לשעבר ראש אגף הטכנולוגיה בשירות הביטחון הכללי.
עו"ד אלי בכר הוא חוקר במכון הישראלי לדמוקרטיה. לשעבר היועץ המשפטי של שירות הביטחון הכללי.

מחיר מומלץ: 45₪
ינואר 2019
מסת"ב:
978-965-519-248-3
0 4500001189 2
דאנאקוד 450-1189
www.idi.org.il