

הגנה על בחירות מפני התערבות זרה במרחב המידע הניסיון האירופי ולקחים לישראל

רעות דוד, עמית כהן, דוד סימן-טוב

אוקטובר 2026

תקציר מנהלים

בשנים האחרונות מסתמן **איום ההתערבות הזרה במרחב המידע**, המוכר במערב בשם Foreign Information Manipulation and Interference (FIMI), כאחד האתגרים האסטרטגיים והביטחוניים המורכבים לדמוקרטיה. בשונה מדיסאינפורמציה לסוגיה, FIMI מתמקד במבצעים מתוזמרים של גורמים זרים המנצלים שסעים חברתיים ופוליטיים ואת סביבת המידע כדי להנדס את השיח הציבורי, להחריף את הקיטוב ולשחוק את אמון הציבור במוסדות הדמוקרטיים ובהליך הבחירות.

מאבק ב-FIMI מחייב ארכיטקטורת חוסן רב-שכבתית. בעוד שהאיחוד האירופי ביסס בעשור האחרון תשתית מוסדית, מתודולוגית ורגולטורית ענפה, ישראל – כפי שעולה מדוח מבקר המדינה שפורסם ביולי 2026 – חשופה לקמפיינים מניפולטיביים זרים בשגרה, בעת מלחמה ובעת בחירות, וסובלת מוואקום כמעט מוחלט של האסדרה בהקשר זה. למעשה, ישראל תלויה ברצון הטוב של הפלטפורמות, משום שחסרים בה תשתית המקבילה ל-Digital Services Act (DSA) – קוד ההתנהגות של האיחוד האירופי בנושא דיסאינפורמציה וחובות שקיפות), מדיניות לאומית מתואמת וגורם מוביל לטיפול מערכתי באתגר ולתיאום אזרחי וממשלתי מוגדר מולו.

מחקר מדיניות זה מציע ניתוח השוואתי של לקחי ההתמודדות של גרמניה, פולין, צ'כיה ומולדובה עם FIMI במהלך מערכות בחירות שנערכו בהן בשנת 2025, לצד מודלים בולטים של התמודדות עם האתגר במדינות נוספות בעולם. **המחקר עשוי להוות בסיס מעשי להיערכות מדינת ישראל לקראת בחירות**, על בסיס הבנה שהניסיון האירופי הוא תשתית ללמידה, ותוך התאמה למאפיינים הייחודיים של ישראל.

המענה המערכתי שהתפתח במדינות אירופה מלמד כי התמודדות אפקטיבית נסמכת על אסדרה מבנית ורב-שכבתית של סביבת המידע כולה. מענה זה כולל ארבעה מאמצים מרכזיים: זיהוי וניטור, רגולציה, תקשורת אסטרטגית ואוריינות דיגיטלית, בשעה שיעילות המענה אינה נגזרת מכלים נפרדים אלא מהשילוב ביניהם.

מנגד, מהניתוח עולים **ארבעה פערים מרכזיים במוכנות הישראלית להתמודדות עם FIMI**: חוסרים רגולטוריים, תלות בשיתוף פעולה וולונטרי מצד הפלטפורמות, פגיעות חברתיות (קיטוב חריף ורמת אמון נמוכה במוסדות) ופגיעות טכנולוגיות.

תובנות מרכזיות שעולות מהמחקר

- המפתח להתמודדות אפקטיבית אינו ריכוז סמכויות אלא **קיום גורם מתאם ואופרטור לאומי קבוע**, הפועל ברציפות בשגרה ובעת בחירות. זהו הפער המוסדי הבולט ביותר בישראל. גוף זה, שיכול להיות חלק מארגון קיים, חיוני להגדרת גבולות ברורים בין ארגוני המודיעין והמדינה לבין החברה האזרחית, כדי למנוע זליגה של סמכויות ביטחוניות חסויות לפיקוח על השיח האזרחי הפתוח.
- מעבר **מרגולציית תוכן לרגולציית התנהגות**: התמודדות יעילה מתמקדת באיתור וסיכול דפוסי פעולה מניפולטיביים, שימוש בחשבונות מזויפים והתנהגות לא אותנטית מתואמת (CIB - Coordinated Inauthentic Behavior), במקום בניסיונות לגבש אסדרה מדינתית של בדיקה מהו מידע אמיתי. התמקדות זו אמורה להגן על חופש הביטוי ולהגביר יכולת למנוע פעילות מניפולטיבית.
- מעבר **מבדיקת עובדות תגובתית להפרכה תקשורתית מטרימה** (Prebanking), המחסנת את הציבור מראש דרך חשיפה מוקדמת של שיטות המניפולציה ממקורות זרים. במישור זה לכלי התקשורת תפקיד כפול: הם יכולים להיות ערוץ יעיל המנגיש את ההסברה המטרימה, אך בהיעדר אחריותיות מקצועית ואימות קפדני הם עלולים לשמש מאיץ ויראלי למסרים זדוניים.

4. שיתוף הפעולה עם הפלטפורמות צריך לעבור **מקשרים אישיים** **אד הוק לערוצים מוסדיים ומחייבים**. הגישה האופרטיבית הנכונה כלפיהן מתמקדת בצמצום חשיפה מראש ומניעת הפצה של הרשתות הזרות טרם חדירתן למיינסטרים, ולא במרדף חסר תועלת אחר הסרת תוכן בדיעבד. קיימים שיתופי פעולה נקודתיים שיש למסדם ולהרחיבם.

5. לצד המדינה, **ארגוני החברה האזרחית** ממלאים תפקיד מכריע בניטור מרחב המידע בזכות עצמאותם היחסית, גמישותם המבצעית וגישתם לרשתות החברתיות. כדי לשמר את עצמאותם נדרש להסדיר את הממשק ביניהם לבין המדינה תוך שמירה על עקרון רגולציית התנהגות בלבד, למניעת פוליטיזציה של המענה המדינתי.

מחקר זה מבהיר כי **ישראל אינה יכולה להסתפק בשיפורים טכניים אד הוק, ונדרשת ארכיטקטורת חוסן לאומית הוליסטית במהותה, שתיגזר מתוך הלקחים והמודלים הבינלאומיים**. עיקריה: הגדרת FIMI כחלק מאיום הייחוס באסטרטגיית הביטחון הלאומי; הקמת גורם מתאם קבוע; התאמת הרגולציה להתנהגות ולא לתוכן; וביסוס שיתוף פעולה בין המדינה, הפלטפורמות והחברה.

חלק מההמלצות, שעל הצורך לפעול לפיהן מצביעות מסקנות המחקר, כבר מבוצעות במידה זו או אחרת בהובלת ועדת הבחירות, גורמי ממשלה וגורמי חברה אזרחית. עם זאת, ייחודו של המחקר הנוכחי הוא בהצגת **גישה שלמה ומערכתית** – שגם אם את חלקה כבר לא ניתן ליישם בפרק הזמן הקצר עד הבחירות – ראוי לאמצה כמצפן למדיניות עתידית בשגרה, ובייחוד בעת בחירות.

תוכן העניינים

3	תקציר מנהלים.....
6	הקדמה.....
9	אתגרי FIMI מגוונים במדינות השונות
9	מהו איום FIMI?.....
9	FIMI כאיום על מערכות בחירות.....
10	האיום הרוסי במערכות הבחירות האירופיות בשנת 2025.....
11	האיום במדינות השונות והמעבר מהתערבות ברשתות למציאות.....
12	פגיעות וחוסן במערכות הבחירות.....
13	התמודדות עם FIMI באירופה
14	ניטור, זיהוי ושיתוף מידע.....
18	חקיקה מול הפלטפורמות הדיגיטליות.....
22	תקשורת אסטרטגית.....
25	אוריינות דיגיטלית וחוסן ציבורי.....
27	מסקנות והמלצות מדיניות לישראל
27	מרחב המידע הישראלי לקראת בחירות אוקטובר 2026: הפערים.....
29	המלצות למדיניות.....
30	המלצות לחברה האזרחית.....
32	סיכום
33	הערות
41	מקורות

המושג FIMI – מניפולציה והתערבות זרה במרחב המידע – מגדיר דפוסי פעולה זרים, מכוונים, מניפולטיביים ומתואמים, הממוקדים בתשתיות הדמוקרטיות עצמן, להבדיל מדיסאינפורמציה המתמקדת באמיתות התוכן.¹ איום ה-FIMI הפך בשנים האחרונות לאחד האיומים המרכזיים על טוהר הבחירות ועל היציבות הדמוקרטית במדינות מערביות.

שחקנים מדינתיים ולא מדינתיים מנצלים את המרחב הדיגיטלי כדי לפגוע במערכות בחירות ובשיח הציבורי הלגיטימי: הפעלת חשבונות פיקטיביים ורשתות לא-אותנטיות; קמפיינים מתוזמרים; התחזות לגורמים פוליטיים או תקשורתיים; והגברה מלאכותית של תכנים ברשתות החברתיות. מטרת הפעילות אינה בהכרח שכנוע ישיר לתמיכה במועמד מסוים, אלא לעיתים קרובות העמקת מחלוקות קיימות, החרפת קיטוב חברתי ופוליטי, טשטוש הגבול בין מידע אמין למידע כוזב ושחיקת האמון בהליך הבחירות ובמוסדות הדמוקרטיים.²

תופעת ה-FIMI מהווה חלק ממגמה גלובלית של התערבות זרה במרחב המידע הדיגיטלי.³ קמפיין ההתערבות הרוסי בבחירות לנשיאות ארצות הברית ב-2016 סימן קו פרשת מים והמחיש כיצד ניתן לנצל רשתות חברתיות, זהויות כוזבות והדלפות מתוזמנות כדי להחרף מתחים פנימיים, לערער אמון במוסדות ולפגוע בשיח הפוליטי הלגיטימי.⁴

אירועים עוקבים במערכות בחירות אירופיות חיזקו את ההבנה כי הגנה עליהן אינה מסתכמת בהגנה טכנולוגית על תשתיות ההצבעה, אלא מחייבת הגנה על מרחב המידע כולו.⁵ האתגר המרכזי שבפניו ניצבות מדינות מערביות דמוקרטיות נובע מהצורך לצמצם מעורבות מדינתית במרחב הציבורי האזרחי, המנוצל על ידי גורמים עוינים.⁶ על כן, נדרש להתמודד חזיתית עם השאלה כיצד לאזן בין הצורך בהגנה מפני האיום החיצוני לבין החשש משימוש לרעה בכוחות ההגנה במישור הפנימי בידי הרוב הפוליטי.

על רקע זה פיתחו מדינות החברות באיחוד האירופי תפיסת הפעלה רב-שכבתית ובין-מוסדית בשיתוף פעולה עם החברה האזרחית, כדי להגן על מרחב המידע תוך צמצום החשש לתופעות לוואי.⁷ תפיסה זו ממוקדת באיום החיצוני ולא בהתערבות בשיח הפנימי, והיא נשענת על אסדרה אזרחית שהתפתחה לקידום ערכים במרחב המידע.⁸ מנגנוני ההתמודדות של האיחוד כוללים ניטור וזיהוי מוקדם, שיתוף מידע בין המדינה לארגוני החברה האזרחית, אסדרת הפעילות במרחב המידע, תקשורת אסטרטגית ואוריינות דיגיטלית.⁹

מטרת מחקר מדיניות זה: לבחון כיצד הניסיון שהצטבר במדינות אירופה בהתמודדות עם FIMI במערכות בחירות יכול לתרום להיערכות לבחירות בישראל.

שאלת המחקר היא: אילו לקחים יכולה ישראל להפיק מהתמודדותן של מדינות אירופה עם FIMI במהלך מערכות בחירות, וכיצד ניתן להתאים לקחים אלה להיערכות לקראת בחירות בישראל?

המחקר מתבסס בראש ובראשונה על דוחות FIMI-ISAC (Information Sharing and Analysis Centre). מודל ה-ISAC, שמקורו בהגנת סייבר, מבוסס על מרכזי שיתוף וניתוח מידע הפועלים כגופים שיתופיים מבוססי אמון ומאפשרים למפעילי תשתיות קריטיות (פיננסים, אנרגיה, בריאות ותקשורת) לשתף אינדיקטורים של תקיפה, לנתח נקודות פגיעות ולגבש פתרונות בזמן אמת, כל זאת באופן מאובטח וחסוי.

החיבור בין עולם הסייבר למאבק ב-FIMI התרחש במסגרת 'המצפן האסטרטגי' של האיחוד האירופי, שהגדיר את המאבק בהתערבות זרה כעוגן.¹⁰ האיחוד זיהה כי מבצעי התערבות מתנהגים באופן זהה למתקפות סייבר וניתנים לפירוק ל"שרשרת תקיפה" (Kill Chain). תובנה זו הובילה להקמת ה-FIMI-ISAC - קואליציה של ארגוני חברה אזרחית, מומחי טכנולוגיה וגופי מחקר המקדמת שיתוף נתונים וסטנדרטיזציה מתודולוגית.¹¹

דוחות FIMI-ISAC מרכזים ידע מקצועי, מקרי בוחן, שיטות ניטור ואמצעי זיהוי וניתוח מגמות רוחביות ודפוסי פעולה של מניפולציה והתערבות זרה במרחב המידע של מדינות אירופה. המחקר מתמקד בניתוח הערכות הסיכון וסקירות שלאחר הבחירות בצ'כיה, פולין, גרמניה ומולדובה במהלך שנת 2025, שמבחינתן רוסיה היא האיום המרכזי.¹² לצד הדוחות, המחקר נשען על מסמכי האיחוד האירופי (European External Action Service – EEAS), פרסומים ממשלתיים, מחקרים אקדמיים ודוחות של ארגוני חברה אזרחית העוסקים בניטור השפעה זרה, בבדיקת עובדות ובחיזוק החוסן הדמוקרטי.

בהתאם לכך, **במחקר זה מיושמת גישה מתודולוגית השוואתית ורוחבית** הכוללת ניתוח מגמות משותפות ושונות בין מודלים של התמודדות, תוך בחינת תפקיד המדינה והחברה האזרחית בחתכי מדיניות שונים. הניתוח מתמקד בארבע מדינות המציגות מודלים מרכזיים: צ'כיה, פולין, גרמניה ומולדובה, שלגביהן קיים תיעוד מקיף ומובנה המאפשר ניתוח השוואתי. לפי הצורך נבחנו מדינות נוספות שראוי ללמוד מניסיוןן.

ייחודו של מחקר מדיניות זה בא לידי ביטוי בשלושה היבטים:

ראשית, **סינתזה רוחבית בין המדינות**: בעוד דוחות FIMI-ISAC המקוריים נכתבו כדוחות הערכה מקומיים ומבודדים, מחקר זה מציע ניתוח אינטגרטיבי הממפה דפוסי פעולה חוצי גבולות. הניתוח חושף כיצד טקטיקות השפעה המנסות ומפותחות במדינות בעלות משאבים מוגבלים ונמצאות בחזית ההתמודדות עם FIMI (דוגמת מולדובה ופולין) עוברות תהליך שכלול מהיר ומיושמות במדינות מפתח באירופה, דוגמת גרמניה.¹³

שנית, **גיבוש מענה מערכתי-תפיסתי לעומת מענה נקודתי**: דוח מבקר המדינה מיולי 2026 חושף כי ישראל פועלת ללא מדיניות לאומית מאושרת, ללא הגדרת אופרטור מוביל וללא תיאום מתכלל קבוע, מה שמוותר את הציבור חשוף למניפולציות מידע עוינות.¹⁴ כשל זה אינו נקודתי או ביצועי אלא תפיסתי, שכן גופי הביטחון, הרגולציה והמשפט בישראל פועלים באורח מבוזר ומקוטע.¹⁵ מחקר זה מתרגם את המענה המערכתי והרב-שכבתי האירופי לארכיטקטורת חוסן אופרטיבית וישימה עבור ישראל, המאחדת את צירי הפעולה השונים.

שלישית, **פתרון ל"שטח המת" הדמוקרטי של גופי המודיעין**: מסקנות המחקר מציעות מענה למתח הדמוקרטי המובנה, שבמסגרתו גופי ביטחון ומודיעין מנועים חוקית, או לעיתים מרסנים את עצמם, מניטור המרחב האזרחי והפוליטי הפנימי מחשש לפגיעה בחופש הביטוי ובאמון הציבור, על בסיס שילוב שכבה אזרחית.¹⁶

הבחירה בניתוח השוואתי נשענת על ארבע נקודות דמיון מבניות, המאפיינות את ישראל והמדינות שנבחנו והופכות את הלקחים המופקים מהן לבעלי ערך יישומי עבור ישראל:

1. התערבות זרה כחלק ממערך היברידי רציף ועקבי: כמו במרבית מדינות אירופה, גם ישראל חווה את ה-FIMI כרכיב קבוע ובלתי נפרד מלוחמה היברידית כוללת המנוהלת על ידי מדינות עוינות.¹⁷

2. קיטוב חברתי עמוק ושבר באמון הציבור במוסדות: מבצעי התערבות מנצלים שסעים קיימים באופן שיטתי כדי לשחוק את האמון במוסדות המדינה.¹⁸ הקיטוב הפוליטי והחברתי בישראל, לצד חוסר יציבות ממסדי, מהווים כר פורה למניפולציה זרה המבקשת להעמיק את השבר הפנימי,¹⁹ בדומה לניצול שסעים דתיים וגיאופוליטיים לטובת מבצעי FIMI בארבע המדינות שנבחנו.²⁰

3. פילוח דמוגרפי ממוקד וקמפיינים מגזריים: המבנה החברתי-דמוגרפי של ישראל, הכולל מגזרים מובחנים בעלי מאפיינים לשוניים ותרבותיים ייחודיים (דוברי ערבית, דוברי רוסית והחברה החרדית), יוצר נקודות פגיעות המבודדות מהשיח הכללי במדינה.²¹ פגיעות דומה זוהתה במולדובה, שבה מבצעי השפעה רוסיים עקפו את הדירקטיבה הלאומית וביצעו מיקרו-טרגטינג לשוני ותרבותי ממוקד מיעוטים, תוך ניצול אוריינות דיגיטלית נמוכה ומחסור בבדיקת עובדות מותאמת.²²

4. הדילמה הדמוקרטית התמזגות האיום הזר בשיח המקומי: במערכות הבחירות באירופה ובישראל כאחת, קמפיינים זרים מתמזגים בשיח הפוליטי הפנימי ומטשטשים את הגבול בין התערבות זרה עוינת לבין ביטוי פוליטי לגיטימי.²³ טשטוש זה מעמיד את גופי הביטחון בישראל ובאירופה בפני מגבלה מבנית זהה: סוכנויות המודיעין מנועות מפיקוח על המרחב האזרחי הגלוי מחשש לפגיעה בחופש הביטוי, מה שיוצר "שטח מת" הגנתי.²⁴

הניסיון האירופי אומנם מציע עקרונות פעולה חיוניים להגנת הבחירות בישראל, אך אלה מורכבים ליישום ישיר עקב מספר הבדלים מבניים. ראשית, בעוד שבאיחוד האירופי ובמדינות נוספות FIMI מוכר כאיום אסטרטגי ואף יש גורם האחראי על תכלול הנושא, בישראל התערבות זרה נמצאת בסדר היום בעיקר לקראת בחירות. שנית, בשונה מהאיחוד האירופי, ישראל פועלת מחוץ ל-DSA (Digital Services Act) וחסרה את כוח המיקוח הכלכלי מול פלטפורמות המדיה. שלישית, ישראל פועלת לבדה וחסרה לה מטריית ההגנה והשיתוף המודיעיני האזורי של מדינות אירופה, ולכן היא נאלצת להתמודד עם האיומים לבדה. רביעית, הקיטוב הפוליטי בישראל יוצר חשדנות מובנת בין המדינה למגזר האזרחי. בעוד שהמודל האירופי של 'חוסן לאומי שלם' (Whole of Society) נשען על אמון הדדי, שיתוף פעולה ותמיכה של המדינה בחברה אזרחית, בישראל קיים מתח מבני: הניטור האזרחי מלווה חשדנות פוליטית, בעוד שגופי הביטחון מנועים בצדק מפעולה במרחב האזרחי הגלוי. לפיכך המענה הישראלי מחייב התאמה של הלקחים למציאות המוסדית והמשפטית המקומית.

במחקר זה נבחנים תחילה מאפייני האיום ודפוסי הפעולה שנצפו במדינות אירופה, ולאחר מכן מאמצי ההתמודדות שלהן בארבעה תחומים: ניטור וזיהוי של פעילות התערבות; פעילות הפלטפורמות והמסגרת הרגולטורית; תקשורת אסטרטגית; ואוריינות דיגיטלית וחוסן חברתי. בכל תחום מזהים חסמים המבניים, הרגולטוריים והמבצעיים שעמדו בפני השחקנים השונים, לצד האסטרטגיות שפותחו על מנת להתגבר עליהם. לאחר מכן מוצגים מרחב המידע, היקף האיום והפערים בהתמודדות הישראלית. לסיום מפורטות מסקנות והמלצות המותאמות למאפיינים הפוליטיים, הביטחוניים והמוסדיים של ישראל, המופנות למדינה ולחברה האזרחית.

אתגרי FIMI מגוונים במדינות השונות

מהו איום FIMI?

התפתחות הפלטפורמות הדיגיטליות והרשתות החברתיות שינתה מהותית את הכלים הנתונים בידי גורמים זרים לשם התערבות בשיח פוליטי ותהליכי בחירות. המרחב הדיגיטלי מאפשר העברת מסרים מהירה ורחבת היקף, התאמה למגוון קהלי יעד, הסוואה של מקור הפעילות ופנייה לקהלי יעד ממוקדים באופן יעיל וזול. על רקע זה התפתח המושג FIMI, המתאר פעילות זרה, מכוונת, מניפולטיבית ומתואמת שמטרתה לפגוע בערכים ותהליכים דמוקרטיים.²⁵ בשונה מדיסאינפורמציה, הבוחנת בעיקר את מידת האמינות של תוכן, FIMI מתמקד בהתנהגות לא אותנטית מתואמת (Coordinated Inauthentic Behavior) – הפעלת רשתות של חשבונות פיקטיביים שמטרתה הטיית השיח הציבורי, זהות התוקף וניסיון להסוות את מקור הפעילות. בהתאם, גם מידע אמיתי הופך לחלק ממבצע התערבות כאשר הוא מופץ באופן מלאכותי ומתואם.²⁶ מטרת העל של מבצעי FIMI אינה שכנוע הבוחרים לתמוך במועמד מסוים או לבצע פעולה מסוימת, אלא העמקת קיטוב, ערעור אמון במוסדות וטשטוש ההבחנה בין מידע אמין לכוזב.²⁷ די ביצירת ספק באמינות ובלגיטימיות של הליך הבחירות כדי לגרום לפגיעה בהליך הדמוקרטי, גם ללא הוכחת שינוי ישיר בתוצאות או בהתנהגות ההצבעה.

מבצעי FIMI נשענים על מגוון טקטיקות, בהן: הקמת רשתות פרופילים מתחזים; ניהול קמפיינים מתוזמרים במספר פלטפורמות במקביל; הגברה מלאכותית של תכנים; שימוש באתרי מראה (אתרים המחקים אתרים אותנטיים) ובדומיינים חלופיים; והצפה במידע. פעולות אלה עשויות לשלב כלי סייבר כגון דיוג (phishing), שיבוש שירותים דיגיטליים, פריצה וגניבה והדלפה של מידע. כלי בינה מלאכותית (AI) מעצימים איום זה על ידי ייצור מהיר וזול של תוכן סינתטי מותאם אישית, המאפשר להפעיל זהויות דיגיטליות רבות במקביל ולהרחיב במידה משמעותית את היקף הפעילות וקצב ההפצה.²⁸

FIMI כאיום על מערכות בחירות

מערכות בחירות מהוות יעד מרכזי לפעילות FIMI בשל רגישותן הציבורית הגבוהה, התחרות הפוליטית האינטנסיבית והצריכה המוגברת של מידע, שבמסגרתה כל אירוע או טענה עלולים להיות מנוצלים מיידית. בתנאים אלה, שחקנים זרים יכולים להשתלב בשיח קיים ולהעצים אותו בלי לעורר מחלוקות חדשות. האיום פועל בשלושה רבדים במקביל: פגיעה ישירה במועמדים, במפלגות או בעמדות מדיניות; החלשת הלכידות סביב סוגיות חברתיות המצויות במחלוקת (דוגמת הגירה, יוקר המחיה וזהות לאומית); וערעור ישיר של אמינות הליך הבחירות עצמו באמצעות הפצת טענות כזב בדבר זיוף, מניפולציה בספירת הקולות או האשמה בכוונה "לגנוב" את הבחירות, שתוקפות ישירות את לגיטימיות ההליך.

קושי מרכזי בהתמודדות עם האיום נובע מהטשטוש המכוון בין FIMI לבין שיח פוליטי פנימי לגיטימי. מחד גיסא, גורמים פוליטיים מקומיים עלולים לאמץ נרטיבים זרים כשאלה משרתים את יעדיהם, כך שפעילות מקומית לגיטימית לכאורה משכפלת מסרים שמקורם זר. מאידך גיסא, שחקנים זרים עלולים להשתמש בגורמים פוליטיים מקומיים כדי להסוות את מקור הפעילות ולהציגה כשיח אורגני. התוצאה היא מרחב אפור, שבו קשה להכריע אם קמפיין הוא זר, מקומי, או שילוב של השניים.

לטשטוש זה נודע גם מחיר מוסדי: גופי המודיעין והסייבר הממשלתיים מוגבלים מבחינה חוקית וערכית בפיקוח על המרחב האזרחי הגלוי ובמתן חוות דעת על הלגיטימיות של תכנים פוליטיים פנימיים, מחשש לפגיעה בחופש הביטוי ובלגיטימיות המוסדות. המיזוג בין FIMI לשיח פוליטי לגיטימי יוצר שטח מת משפטי ומבצעי, שבו גופי המדינה מתקשים לפעול.

התפתחות האיום מומחשת במעבר מההתערבות הרוסית בארצות הברית ב-2016 – שמיקמה את האיום במרכז סדר היום הגלובלי והמחישה את ממדיו²⁹ – לתרחיש הקצה שנרשם בבחירות לנשיאות ברומניה ב-2024, כשבית המשפט החוקתי ביטל את תוצאות הבחירות עקב קמפיין זר שנהנה ממקורות מימון זרים לא-מדווחים. המקרה הרומני מהווה תמרור אזהרה דרמטי למחיר הפגיעה בטוהר הבחירות שמשלמת דמוקרטיה.³⁰

האיום הרוסי במערכות הבחירות האירופיות בשנת 2025

בשנת 2025 ניהלה רוסיה מהלכי התערבות במערכות הבחירות **בפולין, בצ'כיה, בגרמניה ובמולדובה**. מהלכים אלה ננקטו בארבע המדינות על רקע שילוב בין אי-יציבות פוליטית, מתחים גיאופוליטיים (מלחמת רוסיה-אוקראינה, משבר הפליטים שנוצר בעקבותיה, היחסים עם האיחוד האירופי ונאט"ו), שחיקה באמון הציבור בממשלות, במוסדות המדינה ובכלי התקשורת הממסדיים וחשש גובר מפני התערבות זרה. הקמפיינים הותאמו לנקודות התורפה המקומיות בכל מדינה, תוך שימוש בטקטיקות דומות והעצמת מחלוקות קיימות סביב המלחמה באוקראינה, משבר ההגירה והכלכלה, וכן תוך הצגת הממשלות והמוסדות האירופיים כפועלים בניגוד לאינטרסים של הציבור, וכך לערער על ריבונותם.³¹

רוסיה הפעילה מספר מבצעי השפעה מרכזיים בעלי תשתיות טכנולוגיות משותפות:

Doppelgänger היא רשת התערבות המזייפת זהויות של כלי תקשורת לגיטימיים באמצעות דומיינים דומים, כדי להחדיר נרטיבים פרו-רוסיים ואנטי-ממסדיים במסווה עיתונאי אמין.³² לצידה פעל קמפיין Operation Overload, שהתבסס על הצפת כלי תקשורת ובודקי עובדות בכמות גדולה של טענות כזב ותכנים לא-אותנטיים, כדי להעמיס על משאביהם ולפגוע ביכולות הניתוח שלהם.³³ מבצע Storm1516 עשה שימוש בסרטונים מבוזזים ובתוכן סינתטי המתחזים למקורות רשמיים, ורשת Pravda הפיצה תעמולה דרך מאות אתרים מתחזים, וכך הלבילה תכנים של גופי תקשורת רוסיים.³⁴

קמפיינים אלו נשענו על מתווכים ושחקנים מקומיים כדי ליצור מראית עין של תמיכה ציבורית אורגנית ולהקשות על ייחוס להתערבות הזרה.³⁵ כך למשל, בפולין זוהו ניסיונות לגייס אזרחים להפצת נרטיבים זרים ובמולדובה הופעלו רשתות של פעילים בתשלום שקיבלו משימות יומיות להפצה מתואמת של תכנים בין פלטפורמות.³⁶

הפעילות לא הוגבלה לפלטפורמה אחת: קמפיינים עברו בין רשתות חברתיות שונות והשתמשו באתרי מראה ובאגרגטורים – פלטפורמות המרכזות ומפיצות באופן אוטומטי תכנים ממגוון ערוצים דיגיטליים במטרה לשוות להם חזות לגיטימית ולהרחיב את תפוצתם. פיזור זה העניק לקמפיינים שרידות גבוהה ואפשר לפלטפורמות להמשיך לפעול ברציפות גם לאחר חסימת חשבונות, ולהלבין נרטיבים שנוצרו בפלטפורמה אחת כדי להגביר פעילות באחרת.³⁷

זוהו ארבע משפחות נרטיבים שחזרו בכל מערכות הבחירות:

א. ערעור אמינות הבחירות: הפצת טענות על אודות זיוף פתקים, השמדת קולות ומניפולציה מצד המדינה או האיחוד האירופי, כדי לעורר חשד לפני יום הבחירות ולהכין את הקרקע לדחף לגיטימציה של תוצאותיהן. בצ'כיה הוצגה הצבעת הדואר של אזרחים בחו"ל כניסיון ממשלתי לתמרן את תוצאותיהן, בגרמניה הופצו טענות בדבר גריסת פתקים ובמולדובה נטען כי הצבעות הדיאספורה (אזרחים החיים מחוץ למדינה) פוברקו, וכי האיחוד האירופי התערב בהליך הבחירות.³⁸

ב. **דה-לגיטימציה של מוסדות:** הצגת הממשלה, רשויות הבחירות, בתי המשפט והתקשורת כמוסדות מושחתים או כפופים לשחקנים זרים, ואף הצגת מנגנוני ההתמודדות עם דיסאינפורמציה ככלי צנזורה ממשלתיים. נרטיב זה הופיע בארבע המדינות שנבחנו ובלט במיוחד בצ'כיה ומולדובה.³⁹

ג. **אוקראינה, רוסיה והמערב:** הסיוע לאוקראינה הוצג כנטל כלכלי, הפליטים מאוקראינה הוצגו כאיום ביטחוני ונאט"ו והאיחוד האירופי תוארו כגורמים המסלימים את המלחמה ופוגעים בריבונות המדינות.⁴⁰

ד. **הגירה, כלכלה וזהות:** חיבור בין מצוקות כלכליות, מחירי אנרגיה וקליטת פליטים הוצגו כהוכחה לכישלון הממשלה ולבגידה מצד האליטות.⁴¹

האיום במדינות השונות והמעבר מהתערבות ברשתות למציאות

אופי האיום השתנה בהתאם לנקודות התורפה בכל מדינה: בפולין ובגרמניה פעלו בעיקר המערכים הטכנולוגיים המוכרים כ-Operation Overload-i Doppelgänger,⁴² בצ'כיה נוצלו אירועים מקומיים נקודתיים לשחיקת האמון בממשלה ובהליך הבחירות⁴³ ובמולדובה התממש איום היברידי שכלל שילוב של קמפיין AI, רשתות של פעילים מקומיים בתשלום ומימון פוליטי בלתי חוקי, שבו פעילות במרחב המידע השתלבה בלחצים פוליטיים, כלכליים וביטחוניים.⁴⁴ עוצמת האיום נמדדה לא רק בכמות התוכן או במספר החשבונות שפעלו, אלא גם במידת השילוב בין גורמים זרים ומקומיים, ביכולת לעבור בין פלטפורמות ובמידה שבה המסרים הצליחו להשתלב במחלוקות קיימות.

אחד המאפיינים המדאיגים והמובהקים של מבצעי FIMI הוא תרגום מניפולציות דיגיטליות לפעולות פיזיות, חבלה ואלימות במציאות, כלומר מעבר מהמרחב המקוון למרחב הפיזי (Offline Transition -Online-to):

- **תיעול משברי הגירה ללחץ פיזי ודיגיטלי במקביל:** בפולין הוגדרה בלארוס כשחקנית העוינת המדינתית השנייה בגודלה אחרי רוסיה. המשטר בבלארוס ניהל מערכה היברידיה רב־ממדית נגד פולין, שבמסגרתה הוא דחק פיזית מהגרים ופליטים אל מעבר לגבול הפולני (המדינות גובלות ביניהן) כדי ליצור לחץ ואי־ציבות, במקביל לקמפיין דיגיטלי שהציג את ממשלת פולין כמפירה זכויות אדם וחסרת יכולת.⁴⁵
 - **השחתת סמלים לאומיים ופגיעה בקלפיות:** קמפיין רשתי בפולין הניע אזרחים להסיר פיזית דגלי אוקראינה וגרמניה מבנייני ציבור ומקלפיות, בהסתמך על טענות כזב שלפיהן בתי המשפט תומכים בהסרת סמלים זרים, מה שמהווה עבירה פלילית.⁴⁶
 - **מבצעי חבלה פיזיים במסווה של "מחאה אזרחית":** המודיעין הרוסי גייס בגרמניה קבלנים להשחתת מאות כלי רכב ולהדבקת סטיקרים פוליטיים של המפלגה הירוקה, במטרה לפגוע בתדמיתה.⁴⁷
 - **מיסוד מחאות בתשלום ואימוני מהומות אלימות:** פעילים הקימו מחנות אוהלים מול משרדי הממשלה במולדובה ושילמו משכורות למפגינים במטרה לחולל כאוס. במקביל סוכל גיוס אזרחים שנשלחו לעבור אימונים להסלמת הפגנות ולניהול מהומות אלימות בסרביה, בהדרכת גורמים המזוהים עם כוח וגנר הרוסי.⁴⁸
- איומי אלימות והפחדה ממוקדת על בכירים ועל מערכת המשפט:** הסטת השיח המקוון לקריאות פיזיות ישירות לאיומי רצח, לרבות איומים מפורשים בטלגרם לפגוע בחייו של נשיא צ'כיה⁴⁹ ומשלוח זרי אבל ותמונות עריפת ראשים לביתה של שופטת במולדובה.⁵⁰

פגיעות וחוסן במערכות הבחירות

ניתוח מקרי הבוחן מעלה כי הפגיעות של המדינות שנבחנו מול איומי FIMI מתכנסת **לארבעה צירים מבניים**, הגם שקיימת שונות בין המדינות. ראשית, פערים רגולטוריים: פולין וצ'כיה לא השלימו את הטמעת ה־DSA במועד; גרמניה התקשתה לאכוף כללים מול תכנים מזיקים שאינם בלתי חוקיים במובהק; ומולדובה, שאינה חברה באיחוד האירופי, חסרה מעטפת רגולטורית. שנית, תלות בפלטפורמות: היעדר סמכויות אכיפה להסרת תכנים או לחייב מסירת נתונים הותיר את המדינות תלויות בשיתוף פעולה וולונטרי ולא עקבי מצד הפלטפורמות. שלישית, שסעים חברתיים: קיטוב פוליטי, רמת אמון נמוכה במוסדות וחרדות כלכליות סיפקו קרקע פורייה להעצמה ולהחדרה של נרטיבים זרים. רביעית, פגיעות טכנולוגיות: תוכן מבוסס AI, רשתות אוטומטיות ופעילות חוצת פלטפורמות הרחיבו את היקף הפעילות והקשו על זיהוי וסיכול בזמן אמת.⁵¹

לצד נקודות הפגיעות ניתן לזהות **ארבעה גורמי חוסן** במדינות שנבחנו. ראשית, תשתית בחירות עמידה: שמירה על הצבעה ידנית, ספירה מבוזרת ופרסום תוצאות בזמן אמת ברמת המחוז הפחיתו את הסיכון לשינוי תוצאות באמצעות תקיפת סייבר. שנית, מסגרות משפטיות ומוסדיות: מתאמים וחקיקה רלוונטית המרכזים את מאמצי המניעה והסיכול, גם אם חלקית. שלישית, ניסיון מצטבר: פיתוח למידה וזיכרון ארגוני במדינות שחוו מערכות בחירות תכופות אפשרו זיהוי מהיר של דפוסי פעולה של ניסיונות FIMI מוכרים והיערכות לקראתם מראש. רביעית, רשתות ניטור משולבות: שיתוף פעולה מוסדר בין גופי המדינה, החברה האזרחית והפלטפורמות, שיוצר תמונת מצב אחידה ומענה יעיל.⁵²

התמודדות עם FIMI באירופה

ההגנה על מרחב המידע מחייבת **קואליציה רב-מגזרית** המשלבת שירותי ביטחון, רשויות בחירות, גופי סייבר, רגולטורים, משרדי ממשלה, פלטפורמות דיגיטליות (המהוות כאמור גם חלק מהבעיה), ארגוני חברה אזרחית, מכוני מחקר, חוקרים עצמאיים וכלי תקשורת. חלוקת האחריות ביניהם אמורה להשתנות בהתאם למבנה המוסדי, עוצמת האיום, המסגרת המשפטית והמשאבים הקיימים של כל מדינה.

גורם מרכזי להצלחת מערך הגנה זה הוא **גוף מתאם ברמת המדינה**. גוף זה מסנכרן בין הגופים השונים, מונע כפילויות ומשמש ערוץ תקשורת רשמי מול הפלטפורמות. ארבעת מקרי הבוחן מציגים שונות ברמת המיסוד, המיקום והסמכויות של הגורם המתאם במערכות הבחירות ב-2025:

- **גרמניה** – התיאום הרגולטורי במדינה מוסדר באמצעות סוכנות הרשת הפדרלית, הפועלת תחת משרד הכלכלה ומשמשת כמתאם השירותים הדיגיטליים המדינתי מכוח ה-DISA. תפקידה המרכזי הוא פיקוח על עמידת הפלטפורמות בהתחייבויותיהן לצמצום סיכונים בחירות, ותיווך מול חוקרים מהאקדמיה ומהחברה האזרחית. במקביל, ה-BfV (מקביל לשב"כ) שימש כמתאם ביטחוני-מודיעיני באמצעות כוח משימה ייעודי לבחירות.⁵³
- **מולדובה** – הוקם גוף מתאם ייעודי בעל מעמד חוקי עצמאי – המרכז לתקשורת אסטרטגית ולמאבק בדיסאינפורמציה (CSCCD) – שהקים כוח משימה בין-משרדי לליווי ועדת הבחירות המרכזית. המרכז הוסמך בחוק להוביל ולתאם את המענה המדינתי ל-FIMI, והוגדר רשמית כאחראי הלאומי לתיאום מול מטא וגוגל.⁵⁴
- **פולין** – התיאום המוסדי סבל מפיצול ומפער רגולטורי עקב אי-השלמת מינויו של DSC (Digital Services Coordinator) קבוע. משרד הדיגיטל הפולני אומנם יזם את תוכנית-העל 'מטריית הבחירות' (Election Umbrella) לשיפור הגנת הסייבר, אך בהיעדר רגולטור DSA ייעודי, רשת המחקר הלאומית (NASK-PIB) שימשה כאחראית לניטור תכנים ותיאום מול הפלטפורמות.⁵⁵
- **צ'כיה** – משרד התקשורת הצ'כי (ČTÚ) אומנם הוגדר כ-DSC, אך סמכויותיו היו מוגבלות משום שהחוק הלאומי המטמיע את ה-DISA לא אושר בפרלמנט טרם הבחירות. בפועל, משרד הפנים וועדת הבחירות ריכזו את התיאום המדינתי, ניתוח איומי מידע בוצע על ידי המרכז נגד טרור ואיומים היברידיים (CHH) הפועל במשרד הפנים, וסוכנות הסייבר הלאומית (NÚKIB) ריכזה את ההגנה הטכנולוגית.⁵⁶

איור 1 מציג את ארגז הכלים (Toolbox) של האיחוד האירופי להתמודדות עם FIMI, המורכב מארבעה צירי פעולה משלימים היוצרים מעגל תגובה מסתגל, שבו כל ציר מזין את האחרים. הציר הראשון, **מודעות מצבית (Situational Awareness)**, הוא הבסיס – גיבוש מתודולוגיה אחידה, ניטור וגילוי איומים, חקירות OSINT והערכת השפעה. הציר השני, **בניית חוסן (Resilience Building)**, כולל ביסוס תקשורת אסטרטגית, מערכת התרעה מהירה, אוריינות דיגיטלית, חיזוק והעצמת התקשורת העצמאית והחברה האזרחית ובדיקת עובדות. הציר השלישי, **שיבוש ורגולציה (Regulation & Disruption)**, מרכז את הכלים המשפטיים לצמצום מרחב הפעולה של גורמי ההשפעה – החלת ה-DISA, קוד ההתנהגות בנושא דיסאינפורמציה, הטלת חובת שקיפות וחסימת אתרי תעמולה זרים. הציר הרביעי, **פעולה חיצונית (EU External Action)**, מרחיב את ההתמודדות לזירה הבינלאומית: סנקציות, ייחוס פוליטי של תקיפות, קידום נורמות, ותגובה מהירה מתואמת עם שותפים כמו ה-G7.⁵⁷ ארבעת צירי הפעולה מתורגמים לארבעה עמודי תווך של אסטרטגיית Counter-FIMI – זיהוי, מניעה, תגובה ושיתוף פעולה.

איור 1 - ארגז הכלים של האיחוד האירופי בהתמודדות עם FIMI



European Union, "Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)," March 17, 2026. <https://tinyurl.com/4tbf89x9>

ניטור, זיהוי ושיתוף מידע

ניטור מרחב המידע הוא תשתית הכרחית לזיהוי מבצעי FIMI ולתגובה להם. המדינות שנבחנו עברו מניטור מבוזר המבוצע בארגון יחיד למערכי הגנה אינטגרטיביים, המחברים בין שלושה מקורות משלימים: מידע מדינתי ומודיעיני, מחקר ממקורות גלויים של החברה האזרחית ונתונים מפלטפורמות המדיה. כל אחד מהמקורות מספק יכולות ייחודיות, ושילובם חיוני להבחנה בין קמפיין זר מתוזמר לבין פעילות פוליטית מקומית או הפצה בלתי מכוונת של מידע מטעה.

ניטור מדינתי

המדינה מילאה תפקיד מרכזי בזיהוי איומים, בהערכתם ובקישורם לסיכוני סייבר, ריגול ומימון זר, בזכות גישה למידע מודיעיני, סמכות להגן על תשתיות הבחירות ויכולת לתאם בין גופי ביטחון, רשויות בחירות ומשרדי ממשלה. עם זאת, האחריות בארבע המדינות פוצלה בין מספר מוסדות, מה שאפשר לכל גוף להתמקד בתחום המומחיות שלו אך יצר אתגרי תיאום.⁵⁸

- בפולין נבנתה מערכת רב-שכבתית מבוזרת, שפיצלה את הניטור בין סוכנות ביטחון הפנים (ABW, מקבילה לשב"כ), שאבטחה את מרחב הסייבר, לבין מכון המחקר הלאומי (NASK), גוף אזרחי טכנולוגי שניתח דיסאינפורמציה ברשת, וצוות ה-FIMI במשרד החוץ. חלוקה זו אפשרה לטפל במקביל בהגנת תשתיות ובמבצעי התערבות, אך הגבירה את אתגרי התיאום.⁵⁹
- בצ'כיה יושם מודל מבוזר שחילק את האחריות בין שירות המודיעין (BIS, מקביל לשב"כ) שאבחן FIMI, המרכז למאבק באיומים היברידיים (CHH) במשרד הפנים שמיפה נרטיבים וסוכנות הסייבר הלאומית (NUKIB), שהגנה על תשתיות הבחירות ועל רישומי האוכלוסין.⁶⁰
- בגרמניה מסגר שירות ביטחון הפנים (BfV, מקביל לשב"כ) את ה-FIMI כאיום מערכתי על ארון הציבור ועל יציבות המשטר. גישה זו סייעה לגייס תגובה מוסדית רחבה, אך עוררה ביקורת ציבורית בשל מעורבות סוכנות ביון בפיקוח על המרחב האזרחי.⁶¹
- במולדובה התקיים תיאום בין ועדת הבחירות, שירות הביטחון והמודיעין (SIS, מקביל לשב"כ) והמרכז לתקשורת אסטרטגית ומאבק בדיסאינפורמציה (CSCCD – גוף הסברה אזרחי ממשלתי). תיאום זה אפשר ניטור איומים סימולטני, אך נתקל בהיעדר חקיקה פלילית מתאימה ובחוסר שיתוף פעולה מצד הפלטפורמות.⁶²

אל מול מקרי הבוחן המבוזרים, המודל הצרפתי מציג תפיסה הוליסטית ומוסדרת להקמתו של אופרטור תיאום לאומי קבוע.⁶³ בשנת 2021 הוקמה סוכנות VIGINUM – שירות לאומי ייעודי הממוקם במזכירות הכללית להגנה וביטחון לאומי (SGDSN), הכפופה ישירות לראש הממשלה. הסוכנות משמשת כליבת תיאום בין-משרדית באמצעות הובלת הוועדה המבצעית הלאומית וזרועה הטכנולוגית, המאחדות בזמן אמת את קהילת המודיעין, משרד הפנים ומשרד החוץ לשם גיבוש תגובה מהירה ומאוחדת.⁶⁴

ניטור מדינתי אפקטיבי מחייב חיבור בין שלושה רבדים: מודיעין, ניטור והיכרות עם הנרטיבים ועם ההקשר הפוליטי המקומי. היעדר חיבור ביניהם פוגע ביכולת המדינה לבנות תמונת מצב מלאה ולהבחין בין קמפיין זר מתואם, פעילות פוליטית מקומית והפצה בלתי מכוונת של מידע מטעה.

ניטור אזרחי

הצורך בשילוב החברה האזרחית בארכיטקטורת ההגנה הלאומית נובע ממגבלותיהם החוקיות והערכיות של גופי המודיעין והסייבר הממשלתיים, המנועים מפיקוח על המרחב האזרחי והפוליטי עקב חשש לפגיעה בחופש הביטוי ובלגיטימיות המוסדות.⁶⁵ מגבלה זו יוצרת שטח מת כאשר מבצעי התערבות זרים מתמזגים עם קמפיינים מקומיים, הממומנים באופן מוסווה על ידי שחקנים פוליטיים או מוגברים באמצעות שסעים קיימים.⁶⁶ לחברה האזרחית גמישות המאפשרת פרסום ממצאים ללא תלות בהליכים ממשלתיים, במומחיות בשפות ובהקשרים פוליטיים מקומיים ובאמינות ציבורית עצמאית שאינה מזוהה עם הממשלה. בכך **ממלאים ארגוני החברה האזרחית תפקיד משלים לגופי המדינה**. בארבע המדינות פעלו רשתות ניטור אזרחיות, שנבדלו ביניהן במידת המיסוד, בהיקף המשאבים ובמידת שיתוף הפעולה עם המדינה.⁶⁷

ראיית החברה האזרחית במדינות אלו רחבה: היא כוללת קואליציות המאגדות ארגוני מחקר ואקדמיה, גופי בדיקת עובדות, קבוצות מתנדבים וחוקרי OSINT המקיימים קשרים הדוקים ומשלבים לעיתים גם עיתונאים וכלי תקשורת.⁶⁸ קשרים אלו נשענים על טקסונומיות אחידות ובראשן מודל DISARM (Disinformation Analysis and Risk Management), שהוא מסגרת טקסונומית בקוד פתוח המבוססת על תפיסות מעולם הגנת הסייבר למיפוי ולסיווג מבצעי FIMI. המודל מתמקד במיפוי התנהגותי של הטקטיקות, הטכניקות והפרוצדורות (TTPs) שבאמצעותן מבוצע הקמפיין, כדי ליצור שפה משותפת, שיתוף מידע וסיכול אפקטיבי של האיום בין ארגונים ומדינות.⁶⁹

בצ'כיה פעלה רשת ארגונים מבוססת המשלבת קבוצות מתנדבים עצמאיות ("האלפים הצ'כים") המדווחים על התערבות זרה ברשתות, ארגוני בדיקת עובדות וניטור (כגון CEDMO ו-Demagog.cz) המאמתים טענות פוליטיות ומנטרים נרטיבים פוליטיים, וחוקרים טכנולוגיים (Online Risk Labs) שחשפו רשתות השפעה מורכבות.⁷⁰ בגרמניה פעלו קואליציות אזרחיות (כגון רשת FDEI – FIMI Defenders for Election Integrity – Counter Disinformation Network – CDN) שמיפו וחקרו קמפיינים כמו Operation Overload! Doppelgänger, והציגו אותם כמערכ התערבות מתואמת המשלב התחזות, תוכן סינתטי, הגברה מלאכותית ומעבר בין תשתיות, ולא כאוסף של פוסטים נפרדים.⁷¹ במולדובה השתתפו יותר מ-30 ארגוני חברה אזרחית במאמץ ניטור משותף שהפיק 22 התרעות על אירועים מאומתים וחשף את הקשר בין פעילים בתשלום וקמפיינים מקומיים לתשתיות פרו-רוסיות רחבות ולאתרים מתחזים.⁷²

במודל חוסן לאומי שלם (Whole of Society) בפולין פעל צוות התגובה FRT (FIMI Response Team) במסגרת פרויקט FDEI, וייצג את המודל המשולב ביותר שנבחן. הפרויקט איגד 28 ארגונים מקומיים ובינלאומיים ושילב עיתונאים ישירות בצוותי הניטור. שילוב זה אפשר לתרגם את הממצאים במהירות לתוכן ציבורי – עשרות מאמרים, שידורי רדיו וסרטונים שהגיעו למאות אלפי אזרחים – ולהפיק חקירות מפורטות של תקריות ב-20 מאמצי התערבות שונים. נוסף על כך, באמצעות מערכת התגובה המהירה של האיחוד נוצר ערוץ ישיר להעברת מקרי CIB ישירות לפלטפורמות.⁷³

למרות תרומתה, החברה האזרחית אינה תחליף למדינה אלא גורם משלים חיוני. לארגונים אזרחיים אין גישה למידע מסווג, לנתוני עומק של הפלטפורמות או לסמכויות אכיפה, ויכולתם תלויה במימון (שלעיתים ניתן על ידי המדינה), בגישה לפלטפורמות ובנכונות הרשויות לקבל את ממצאיהם. פעילותם מלווה במתחים מובנים: קושי של המדינה לחלוק עימם מידע מסווג, היענות חלקית מצד הרשתות החברתיות ותחרות פנימית בין הארגונים על תקציבים, המקשה על שמירת רציפות הניטור לאורך זמן. עם זאת, יתרונם העיקרי הוא בניטור פתוח, במחקר, בהנגשת מידע וביצירת לחץ ציבורי ומוסדי.⁷⁴

מנגנונים משולבים

המודלים האירופיים לא הפרידו בין המדינה לחברה האזרחית, אלא בנו ערוצי שיתוף פעולה בין-מגזרי המבוסס על יתרונות משלימים: המדינה סיפקה מידע רשמי, סמכות וגישה, החברה האזרחית סיפקה ניטור פתוח, גמישות ומומחיות מקומית, כלי התקשורת הנגישו ממצאים לציבור והפלטפורמות החזיקו בנתונים וביכולת לצמצם הפצה. פריצת הדרך המבצעית הושגה במעבר מניטור תכנים נקודתי ותגובתי לשיתוף מודיעין התנהגותי וטקטי על הרשת כולה. במקום להתווכח על לגיטימיות של פוסט יחיד, הגורמים משתפים חתימות דיגיטליות: דפוסי פתיחת חשבונות ורשתות בוטים, רשימות דומיינים מזויפים, קשרים בין פלטפורמות, תזמון פעילות וייחוס.

מיקוד טכנולוגי זה מעלה דרמטית את שיעור חסימת האיומים ומגביל את הפצתם, ומקצר במידה רבה את זמני התגובה. יתרה מכך, הוא פותר את כשלי היסוד של המענה הדמוקרטי: הוא עוקף את המתח הפוליטי באמצעות התמקדות בהתנהגות ומאפשר לפלטפורמות להחיל חסימות אוטומטיות מבוססות תשתית בקנה מידה רחב.⁷⁵

שילוב ארגונים אזרחיים ומתנדבים בארכיטקטורת ההגנה הלאומית על מרחב המידע הוסדר במדינות השונות באמצעות שלושה מנגנונים עיקריים: ראשית, הענקת מעמד עצמאי של 'מדווחים אמינים' (Flaggers Trusted – גופים עצמאיים המוסמכים על ידי הרגולטור הלאומי מכוח סעיף 22 ל-DSA, שדיווחיהם על אודות הפרת כללי הקהילה או פעילות מניפולטיבית זוכים לקדימות ולטיפול מועדף ומיידי מצד הפלטפורמות) – בגרמניה ובצ'כיה הרגולטור מעניק לארגונים אזרחיים מעמד מועדף, המאלץ את הפלטפורמות להעניק עדיפות אחיפה מיידית לדיווחיהם.⁷⁶ שנית, תיאום בין קבוצות מתנדבים אזרחיות, המנוהל באופן ריכוזי מול גורמי מחקר וסייבר ממשלתיים (כמו רשת המחקר הלאומית NASK בפולין). שלישית, גופי תיווך אזרחיים-ממשלתיים: שימוש במרכז לתקשורת אסטרטגית ולמאבק בדיסאינפורמציה (CSCCD) במולדובה כגוף אזרחי-ממשלתי המרכז את ממצאי הניטור האזרחי ומעבירים לוועדת הבחירות, וכך מונע מעורבות ישירה של סוכנויות הבין בשיח הציבורי.⁷⁷

בגרמניה ובמולדובה הופעל מנגנון Incident Alerts – מערכות התרעה שהעבירו בזמן אמת דיווחים מפורטים לגורמי בחירות, רגולטורים, פלטפורמות בודקי עובדות וכלי תקשורת על אודות דפוס הפעולה, הערכת ההשפעה האפשרית והמלצות לתגובה. במולדובה לווח המאמץ בתרגילי מוכנות ומבחני מאמץ משותפים למדינה, לחברה האזרחית ולשותפים בינלאומיים, שבחנו תרחישי קיצון של דיסאינפורמציה, מתקפות סייבר ופגיעה בתשתיות הבחירות.⁷⁸

המודל הצ'כי הדגים כי שיתוף פעולה לא מחייב הקמת גוף ריכוזי, אלא יכול להתבסס על רשת גמישה שבה כל גורם שומר על עצמאות תוך העברת מידע בערוצים מוסדרים. כך למשל Online Risk Labs, מעבדת מחקר לסיכונים דיגיטליים, חשפה רשת חשבוניות והעבירה את הממצאים לשירות המודיעין (BIS). החשבוניות הועברו למשרד התקשורת, שפנה לטיקטוק וגרם להסרה של חלק מהחשבוניות בגין הפרה של כללי השירות. זאת ועוד, Demagog.cz פעל כמדווח אמין עבור מטא, ולכן היה מסוגל להעביר דיווחים ישירות ולקבל מענה מהיר, כאשר חודש לפני הבחירות במדינה נפתחו ערוצים ישירים גם מול גוגל ומיקרוסופט.⁷⁹

מגבלות הניטור

למרות הרחבת היכולות, בכל המדינות נותרו ארבע מגבלות ניטור מרכזיות:

1. נתק מבצעי בין שלב הניטור והאבחון לשלב התגובה והסיכול: לגופי הניטור הממשלתיים והאזרחיים כאחד

חסרו סמכויות אחיפה וכלים טכנולוגיים ישירים לעצירת המניפולציות ברשת. הגופים שזיהו איומים בפולין ובצ'כיה יכלו להפיק התרעות בלבד, אך נתקלו בחסם מובנה מול הפלטפורמות שלא היו מחויבות חוקית לפעול. היעדר יכולת אחיפה עצמאית במולדובה הותיר את יכולת הניטור תלויה בנכונות הפלטפורמות.⁸⁰

2. עומק ניתוח מוגבל בשל גישה מצומצמת לנתוני פלטפורמות: חוקרים וגופי מדינה

נאלצו לפעול לרוב על בסיס מידע ציבורי גלוי בלבד – נתונים על הפצת תוכן, מימון פרסום, זהות מפעילי החשבוניות וקשרים פנימיים בין משתמשים נותרו בידי החברות.⁸¹

3. הקושי להבחין בין FIMI לשיח פוליטי פנימי: מבצעי התערבות משתלבים באופן מכוון בשיח הפוליטי הפנימי, מה

שמקשה על סימונם כפעילות עוינת. בפולין אימצו שחקנים פוליטיים מקומיים טקטיקות המזוהות עם מבצעי התערבות זרים; בצ'כיה ניצלו גורמי התערבות תקריות שמקורן בטעות אנוש או בהונאה פלילית; ובמולדובה גויסו פעילים ומשפיענים מקומיים, והופעלו אתרי חדשות ותקשורת מזויפים שהתחזו לגופי חדשות לגיטימיים והפיצו נרטיבים פרו-רוסיים.⁸²

4. **הפיכתם של מנגנוני הניטור יעד למתקפה:** שחקנים עוינים פיתחו שיטות לשיבוש מנגנוני הניטור עצמם. מבצע Operation Overload הציף חוקרים ובודקי עובדות בכמות גדולה של תכנים כוזבים, כדי להעמיס על משאביהם ולפגוע ביכולת לתעדף איומים. נוסף על כך, חשיפת קמפיין לא הובילה בהכרח לעצירתו, אלא גררה מעבר מהיר וגמיש לדומיינים ולתשתיות חלופיות.⁸³

חקיקה מול הפלטפורמות הדיגיטליות

הפלטפורמות הדיגיטליות הן הזירה המרכזית שבה מתבצע FIMI, אך גם גורם חיוני בהתמודדות עימו: הן מחזיקות במידע על אודות המשתמשים, רשתות ההפצה, פרסום ממומן ודפוסי התנהגות, וכן ביכולת להסיר חשבונות, לצמצם תפוצה ולשנות מנגנוני המלצה.⁸⁴ ואולם הפלטפורמות פועלות מתוך ניגוד אינטרסים מובנה – המודל העסקי שלהן מתגמל מעורבות (engagement) והפצה נרחבת, כך שתכנים מעוררי פחד וכעס זוכים להפצה מוגברת גם כשמקורם אינו אמין.

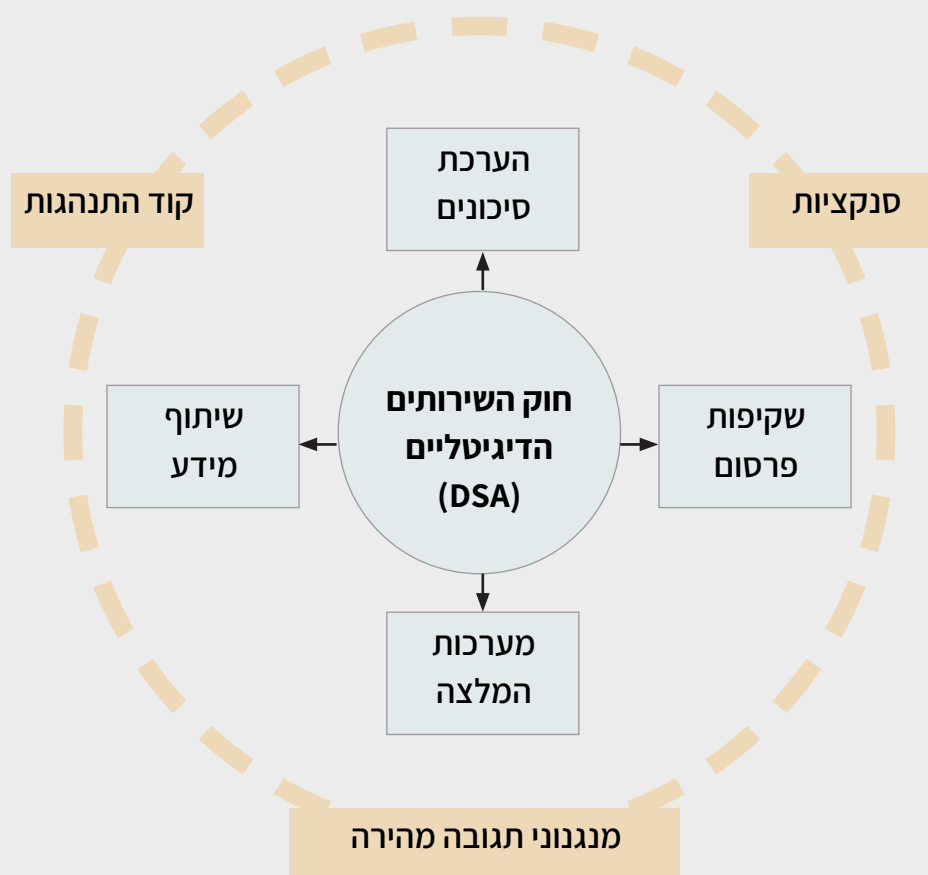
מאפיין זה בא לידי ביטוי בקלות היתר של פתיחת חשבונות רבים ב-X, אכיפה לא אחידה במטא, התרת פעילות בחשבונות לא מאומתים ולקות בזיהוי מקור המימון בפרסום דיגיטלי בטיקטוק. יתרה מכך, קמפיינים זרים מפגינים גמישות גבוהה ומדלגים במהירות בין תשתיות – דרך אתרי מראה, פרוקסי, ערוצים סגורים ותכנים סינתטיים – באופן המקשה על בודקי עובדות, מנטרל חסימות ועוקף סנקציות. בשל כך, הניסיון האירופי עבר בהדרגה מהסתמכות על התחייבויות וולונטריות של הפלטפורמות למסגרות חוקיות מחייבות של שקיפות, פיקוח והערכת סיכונים, אם כי עם פערי יישום משמעותיים בין המדינות.⁸⁵

המסגרת הרגולטורית האירופית

המענה המערכתי הרגולטורי של האיחוד האירופי נולד מתוך הבנה כי טיפול תגובתי מוביל למבוי סתום בהתמודדות עם איומי מידע. הוכחה דרמטית לכך היא משבר הבחירות ברומניה: בהיעדר תשתית רגולטורית מונעת ומבוססת אכיפה מול הפלטפורמות בזמן אמת, המדינה נאלצה להגיב רק לאחר מעשה בצעד הקיצוני של ביטול תוצאות הבחירות.⁸⁶ חוק השירותים הדיגיטליים האירופי (DSA) נועד למנוע משבר כזה בדיוק, על ידי מעבר לאסדרה מערכתית מונעת ומסגרת להתמודדות עם סיכונים מערכתיים לפגיעה בטוהר הבחירות בפלטפורמות דיגיטליות.⁸⁷ במקום להתמקד בחסימת תכנים בלתי חוקיים נקודתיים, החוק מטיל על הפלטפורמות חובות בארבעה תחומים:

- הערכת סיכונים – חובה לזהות ולצמצם סיכונים מערכתיים הקשורים לבחירות לפני מועד ההצבעה.⁸⁸
- שקיפות בפרסום – חשיפת זהות מממני פרסום פוליטי ומאגר פרסומות נגיש לציבור.⁸⁹
- מערכות המלצה – מתן אפשרות למשתמשים לבחור מערכת המלצה שאינה מבוססת פרופיל.⁹⁰
- שיתוף מידע – מתן גישה לחוקרים ולרשויות לנתוני הפצת תוכן ופרסום ממומן.⁹¹

איור 2 - אקוסיסטם ההתמודדות האירופי



ה-DSA מהווה עוגן משפטי בתוך אקוסיסטם הכולל רגולציה קשיחה על פלטפורמות שאינן עומדות בהתחייבות, קוד התנהגות בנושא דיסאינפורמציה, התחייבות מרצון של הפלטפורמות, מנגנוני תגובה מהירה של רשויות המדינה, האיחוד האירופי והחברה האזרחית, וכן סנקציות על כלי תקשורת רוסיים המפיצים תעמולה.⁹² ואולם הניסיון האירופי מוכיח כי מעטפת רגולטורית משפטית זו אינה יכולה לפעול בחלל ריק, והיא מחייבת מנגנון יישום מוסדי.

תפקידו המרכזי של גוף מתאם אינו רגולטורי בלבד, אלא כולל קביעת מדיניות אחידה וסנכרון המאמצים המדינתיים והאזרחיים ברציפות בשגרה ובעת בחירות. ללא גוף ייעודי המוביל מדיניות לאומית מול איומי התערבות, המתאם בין הגופים ומעניק סמכויות ברורות, החקיקה מתקשה להתמודד עם קמפיינים המתפתחים במהירות.

יתרון מרכזי של המסגרת הזו הוא שמדינות אינן נדרשות להתמודד לבדן עם חברות טכנולוגיה גלובליות, אלא היא מאפשרת לנציבות האירופית, למתאמי השירותים הדיגיטליים ולרגולטורים הלאומיים לפעול במסגרת כללים משותפת. באופן זה נוצרת רגולציה תשתיתית של השוק הדיגיטלי ומרחב המידע. בגרמניה למשל תמכו ה-DSC, הנציבות וה-DSC הלאומי בתיאום בין רשתות ניטור, ויצרו מנגנון המאפשר לממצאים להגיע לרגולטורים ולפלטפורמות בערוץ מוסדי.⁹³ עם זאת, החקיקה אינה מבטיחה יישום אחיד, ויעילותה תלויה בהשלמת חקיקה לאומית, בקיומו של רגולטור מוסמך ובנכונות הפלטפורמות לפעול, ולכן נוצרו פערים משמעותיים בין המדינות.

אל מול הגישה האירופית, המעדיפה מנגנונים של ניהול סיכונים מערכתיים ואחריותיות מבוזרת, המודל הסינגפורי מייצג גישה שונה – אסכולת האכיפה הריבונית הקשיחה (Hard Regulatory Enforcement). באמצעות חוק FICA (Foreign Interference Countermeasures Act) עברה סינגפור מתפיסה של בקשת מחוות וולונטריות מהפלטרמות לפעולה על סמך סמכות כופה המעוגנת בחוק. חקיקה זו מעניקה לרשויות המדינה את הכוח המשפטי להוציא צווים מנהליים מהירים, המאלצים את הפלטרמות להסיר פרסומים באופן מיידי, לחסום חשבונות פיקטיביים ולחשוף את זהות המממנים של קמפיינים פוליטיים ברשת. המודל ממחיש כי הגנה אפקטיבית על טוהר הבחירות מחייבת לעיתים סל כלים משפטי המעגן סמכויות אכיפה שלטוניות ישירות כלפי ענקיות הטכנולוגיה, ולא רק הסתמכות על התחייבות מרצון של הפלטרמות.⁹⁴

פערי יישום ברמה הלאומית

הצלחת הרגולציה האירופית תלויה ביכולת המדינות לתרגם את המסגרת לסמכויות ולמנגנוני אכיפה לאומיים. הגדרת FIMI כאיום ייחוס באסטרטגיית הביטחון הלאומי מעניקה מנדט לגופי הביטחון, ותרגומה לחוקים חיוני להקניית סמכויות אכיפה מול הפלטרמות במרחב האזרחי. למרות זאת, הפערים המבניים בין ארבע המדינות שנבחנו משתקפים בטבלה הבאה:

מדינה	מצב ה-DSA והמסגרת החוקית	פערים רגולטוריים וחסמים מרכזיים	השלכות מבצעיות ודוגמאות בשטח
פולין	הטמעה חלקית בלבד; לא פעל במדינה DSC מוסמך, מה שהגביל את פיקוח המדינה על סיכונים ועל פעילות הפלטרמות.	FIMI לא הוגדר בדין הלאומי; היעדר רגולציה ייעודית להתמודדות עם תוכן מבוסס AI ומימון זר של קמפיינים.	יכולת מוגבלת מאוד של המדינה לרכז מידע על איומי רשת ולהגיב עליהם באופן רוחבי ומתואם.
צ'כיה	ההטמעה לא הושלמה במועד – החוק הלאומי המטמיע את ה-DSC לא אושר בזמן בפרלמנט; הנציבות האירופית פתחה בהליכים נגד צ'כיה בגין הפרה.	משרד התקשורת חסר סמכות אכיפה וענישה למרות שהוגדר כמתאם; חסרה חקיקה ייעודית ל-FIMI.	פגיעה ביכולת האכיפה הישירה – במקרים של חסימת אתרים פרו-רוסיים נאלצה הממשלה להסתמך על פניות וולונטריות א-פורמליות לספקי אינטרנט מקומיים.
גרמניה	מסגרת מפותחת יחסית – סוכנות הרשת הפדרלית תפקדה כ-DSC והפעילה סמכויות פיקוח.	קושי מובנה באכיפה מול תוכן מזיק אך שאינו בלתי חוקי במובהק, מעבר של שחקנים לתשתיות דיגיטליות עוקפות.	קמפיין השפעה מתואם ומזיק יכול לפגוע באמון הציבור באופן מערכתי, גם כאשר כל פרסום יחיד נותר חוקי.
מולדובה	אינה כפופה ל-DSC – היא לא חברה באיחוד האירופי, ולכן לא נהנית מהמטרייה הרגולטורית או מכוח המיקוח הקולקטיבי מול הפלטרמות.	היעדר מסגרת חוקית מחייבת ואכיפה מול הפלטרמות הגלובליות, משאבים ממשלתיים מוגבלים.	פגיעה קשה ביכולת האכיפה הממשלתית, מנגנוני ניטור ותגובה תלויים בשיתוף פעולה וולונטרי של פלטרמות ובסיוע חיצוני.

התמודדות עם FIMI יוצרת מתח מובנה בין הגנה על הבחירות לשמירה על חופש הביטוי ותחרות פוליטית פתוחה. מתח זה נובע מכך שקמפיינים זרים אינם נשענים בהכרח על תוכן שקרי או בלתי חוקי, אלא על הפצת תוכן לגיטימי באמצעות התחזות, תיאום והסתרת המקור. פרסום יחיד יכול להיות חוקי כשלעצמו, בעוד שהמערך המתואם, שבאמצעותו הוא מופץ, יוצר סיכון לדמוקרטיה. לכן, הניסיונות להתמודד עם התופעה באמצעות בחינת מהימנות התוכן בלבד אינם מספקים מענה מלא, ואילו הענקת סמכות רחבה מדי למדינה לקבוע מהו מידע לגיטימי עלולה להוביל לצנזורה או לפגיעה באופוזיציה.⁹⁵

בעוד חסימת אתרים וחשבונות עשויה לצמצם חשיפה בטווח הקצר, ללא שקיפות מספקת היא עלולה לדחוף את הפעילות לערוצים סגורים ולהפוך בעצמה לבסיס של צנזורה ממשלתית. במולדובה למשל, דילמה זו התעוררה סביב צעדים נגד מפלגות, מתמודדים ורשתות, שנחשדו במימון בלתי חוקי או בקשרים עם גורמים זרים. צעדים אלה נועדו להגן על הבחירות, אך חלקם עוררו שאלות בדבר מידתיות ופולרליזם פוליטי.⁹⁶ לכן המענה המשפטי צריך להתבסס על הגדרות ברורות, פיקוח עצמאי, שקיפות והבחנה בין תוכן פוליטי לגיטימי לבין פעילות זרה מתואמת ומוסתרת.⁹⁷ נדרש להתמודד באופן ישיר עם השאלה כיצד לאזן בין הצורך בהגנה מפני האיום החיצוני לבין החשש משימוש לרעה בכוחות ההגנה במישור הפנימי בידי הרוב הפוליטי. מתח זה ניכר בבחירות ברומניה בשנת 2024, כאשר החלטת בית המשפט החוקתי לבטל את הבחירות בשל מניפולציה ממקור זר עוררה פולמוס חריף והאשמות בצנזורה שלטונית.⁹⁸ אירוע זה תורגם מיידית לנשק תודעתי במערכות הבחירות בצ'כיה ובפולין, שבהן שחקנים עוינים הפיצו נרטיב שלפיו הממסד המקומי נערך לבטל את הבחירות באותו אופן.⁹⁹

כדי למנוע מדרון חלקלק זה של פגיעה בחופש הביטוי, המודל הצרפתי מציע פתרון מוסדי ייחודי המאזן בין צורכי הביטחון לחוסן הדמוקרטי: פעילות הניטור של סוכנות VIGINUM הממשלתית כפופה באופן מנדטורי לוועדה ציבורית עצמאית לאתיקה ומדע המורכבת משופטים, חוקרים באקדמיה ואנשי תקשורת. הוועדה מפקחת ברציפות על איסוף הנתונים, מבטיחה כי הניטור אינו גולש לפיקוח על השיח הציבורי הפנימי ומגישה דוחות שוטפים לציבור. יתרה מכך, המענה הצרפתי מפריד באופן מוחלט בין זיהוי האיום לבין הטלת סנקציות: VIGINUM אינה מוסמכת להסיר תכנים. היא מעבירה את ממצאיה הטכנולוגיים לרשות התקשורת והרגולציה האזרחית, הממנפת את כלי ה-DSA לחקירה ואכיפת ניהול הסיכונים של הפלטפורמות בלי לערב זרועות ביטחוניות חשאיות בשיח האזרחי.¹⁰⁰

פעילות הפלטפורמות ושיתוף הפעולה עימן

שילוב הפלטפורמות במערך ההגנה הלאומי מתבסס על דיווח מוסדר של CIB, הגבלת תפוצה, הסרת רשתות וסירוב לפרסום מטעה, תוך שימוש במעמד של מדווחים אמינים.

בפולין השתמש צוות התגובה ל-FIMI במערכת התגובה המהירה של האיחוד האירופי כדי להעביר לפלטפורמות רשתות CIB בערוץ ישיר, וכך עקף את מנגנוני הדיווח הרגילים, שלעיתים היו איטיים או התייחסו לכל חשבון בנפרד בלי לזהות את הרשת הרחבה.¹⁰¹ בצ'כיה פעל ארגון Demagog.cz כגורם מדווח אמין עבור מטא, והוא סייע בזיהוי מהיר של תכנים שעברו מניפולציה. הארגון שיתף פעולה עם מנוע החיפוש המקומי Seznam.cz, שסירב לפרסם מודעות פוליטיות הכוללות טענות שזוהו ככוזבות או מטעות. במקרה נוסף הועברה לטיקטוק רשימת חשבונות אנונימיים שפעלו באופן מתואם, וחלקם הוסרו בעקבות הפרת מדיניות השירות.¹⁰²

בגרמניה, אחרי שהפלטפורמה Bluesky קיבלה דוחות מפורטים על אודות דפוסי הפעולה ושיטות ההתחזות של רשת Doppelgänger, היא נקטה צעדי מיתון מהירים שהובילו לירידה משמעותית בפעילותה.¹⁰³ בתקופת הבחירות במולדובה

אפשר שיתוף פעולה בין הרשויות, החברה האזרחית והשותפים הבינלאומיים העברה מהירה של מקרים מאומתים לפלטפורמות, וביניהן גוגל, מטא וטיקטוק, לצורך חסימה מיידית של רשתות CIB. עם זאת, בהיעדר מסגרת מחייבת דוגמת ה-DSA, יכולתה של המדינה לכפות טיפול מהיר ועקבי נותרה מוגבלת ותלויה ברצון הטוב של החברות.¹⁰⁴

מקרים אלה מלמדים כי שיתוף פעולה עם הפלטפורמות אפקטיבי יותר כאשר הוא מתבסס על ערוצים קבועים, על גורמים מקצועיים ועל סטנדרטים משותפים לתיעוד. דיווח על הרשת, התיאום בה ושיטת הפעולה שלה יעילים יותר מדיווח ציבורי לגבי פרסום יחיד, שאינו מותאם לזיהוי מבצעי FIMI נרחבים ועל כן יזכה לפחות התייחסות מהפלטפורמות.

תקשורת אסטרטגית

תקשורת אסטרטגית היא רכיב חיוני בהתמודדות עם FIMI, שכן מבצעי התערבות מכוונים לערער את האמון הציבורי במקורות המידע ובמוסדות המדינה. תגובה להתערבות זרה אינה יכולה להסתכם בהסרת תוכן – היא מחייבת לספק לציבור מידע אמין, מהיר ונגיש, להסביר את הליך הבחירות ולהכין את הציבור מראש לסוגי המניפולציה הצפויים.¹⁰⁵

הפרכה מטרימה: Pre-bunking

המגמה המרכזית שנצפתה במדינות שנבחנו הייתה מעבר מגישה תגובתית (הפרכת שקרים בדיעבד) לגישה פרואקטיבית של הפרכה מטרימה (Pre-bunking), המכינה את הציבור לאיום בטרם חדירתו למיינסטרים.¹⁰⁶

- בפולין הסבירה הממשלה מראש על מבצעי התערבות רוסיים ועל שיטות פעולה, תוך מינוף הזיכרון המוסדי מרצף מערכות בחירות בשנים הקודמות לזיהוי דפוסים ולאזהרה מפני האיום. הקדמת ההפרכה סימנה שיפור ביחס לבחירות קודמות, שבהן התגובה הייתה מאוחרת.¹⁰⁷
 - בצ'כיה שילבו מהלכי התקשורת האסטרטגית מסר ביטחוני עם חיזוק אמון: BIS הזהיר מראש מפני התערבות זרה, ובימים שלפני ההצבעה נשא הנשיא פטר פאבל נאום לאומה, שקרא לציבור לא להיכנע לניסיונות התערבות רוסיים והדגיש את שקיפות הליך הבקרה והמניעה.¹⁰⁸
 - בגרמניה פרסם ה-BfV מראש הערכת איום מפורטת בדבר דיסאינפורמציה, מתקפות סייבר, ריגול וחבלה פיזית, וכך האיום מוסגר כחלק ממאמץ נרחב לפגיעה בדמוקרטיה, ולא כוויכוח נקודתי לגבי אמיתות תוכן.¹⁰⁹
 - במולדובה הופצו תוכני הפרכה מטרימה בזמן אמת על אירועי FIMI, לרבות הערכת התערבות והמלצות לתגובה, במקביל לתרגילים משותפים שהכינו את הגורמים הרלוונטיים לתרחישי קיצון.¹¹⁰
- להפרכה מטרימה יתרון ברור: הפחתת אפקט ההפתעה וחיזוק יכולת הציבור לזהות שיטות פעולה. עם זאת קיים צורך בדיוק ובמידתיות – אזהרות כלליות או מופרזות עלולות ללבות חרדה או לשחוק בעצמן את האמון בהליך הבחירות.¹¹¹

חלק ניכר מהתקשורת האסטרטגית התמקד בהסבר יזום של פעולת מערכת הבחירות: הצבעת דואר, פתקי הצבעה, ספירת קולות ותקלות במערכות מידע – זאת כדי לשלול מראש נרטיבים של דה-לגיטימציה ו"גניבת קולות".¹¹²

בצ'כיה נדרש הסבר מקיף על הצבעת הדואר לאזרחים בחו"ל, שהוצגה בנרטיבים רוסיים כניסיון ממשלתי לתמרן את התוצאות: משרד החוץ קיים דיונים מקוונים ופרסם סרטונים ומסמכים, משרד התקשורת הסביר לציבור על זכויותיו תחת ה-DSA, והממשלה הבליטה את החוסן של ספירת הקולות הידנית והמבוזרת ופרסמה את תוצאות הבחירות בזמן אמת.¹¹³

בגרמניה הועברו ממצאי רשתות הניטור לגופי בחירות, בודקי עובדות וכלי תקשורת בזמן אמת, כדי להבהיר את שלבי ההליך לציבור ולספק מענה מיידי לטענות כזב בדבר זיוף פתקים, גריסתם ומחסור מכון בפתקי הצבעה.¹¹⁴

גם במולדובה התמקדו חלק מהנרטיבים בדה-לגיטימציה של תוצאות הבחירות, ולכן ועדת הבחירות נדרשה לספק מידע שוטף על תפקוד המערכות ועל ניסיונות למתקפות סייבר, וכן להבהיר כי אלו לא פגעו בהצבעה או בספירה.¹¹⁵

החברה האזרחית והתקשורת

נדרשת הבחנה מושגית בין תקשורת אסטרטגית-מושג המכוון למוסדות מדינתיים ומיועד לקדם יעדי ביטחון לאומי מוגדרים, לבין פעילותם העצמאית של החברה האזרחית והעיתונות. אלה משמשים מקור אימות עצמאי שאינו מזוהה עם השלטון-ועשוי להוות עוגן קריטי במדינות שבהן רמת אמון הציבור בממשלה נמוכה או מקוטבת.¹¹⁶ בהקשר זה, לתקשורת תפקיד מתווך בעל פוטנציאל דו-כיווני: היא מהווה מכפיל כוח להפצת מידע מאומת המחסן את הציבור, אך בהיעדר אחריות מקצועית ואימות קפדני היא עלולה להפוך למאיצה של הדחף תעמולה זרה.¹¹⁷

בפולין שילב צוות התגובה המהירה (FRT) עיתונאים מכלי תקשורת מרכזיים ישירות ברשתות הניטור. שיתוף פעולה זה הניב עשרות מאמרים, שידורי רדיו וסרטונים, שהגיעו למאות אלפי אזרחים והבטיחו שמודיעין האיומים יתורגם למידע ציבורי נגיש במקום להישאר ברשת סגורה.¹¹⁸ בצ'כיה השיקו כלי תקשורת עצמאיים פרויקטים לאימות מידע בשיתוף בודקי העובדות CEDMO ו-Demagog.cz, שחשפו רשתות בטיקטוק ובטלגרם ופרסמו תחקירים מפורטים – מהלך שהציג שילוב בין ניטור מחקרי, בדיקת טענות והנגשה תקשורתית.¹¹⁹ בגרמניה פרסמו ארגוני חברה אזרחית התרעות ודוחות מפורטים, שסייעו לעיתונאים לזהות רשתות של תכנים שנראו אותנטיים ובכך תרמו לשקיפות.¹²⁰ במולדובה עבדו עיתונאים וחוקרים עם שותפים בינלאומיים לחשיפת רשתות הפצה, פעילים בתשלום ואתרים מתחזים, וסיפקו לציבור מידע שלא היה זמין בערוצים הממשלתיים.¹²¹

כדי לשמר את אמינותם הציבורית, על כלי התקשורת והחברה האזרחית לשמור על עצמאות מן המדינה. מודל אפקטיבי מחייב תיאום עובדתי ושיתוף מידע על איומים, לצד שמירה על עצמאות מערכתית וחלוקת תפקידים ברורה.¹²²

הניסיון המצטבר חושף חמישה כשלי יסוד ביישום תקשורת אסטרטגית:

1. הגורם המפריך אינו זוכה בהכרח לאמון הקהל שנחשף למידע המטעה: בצ'כיה, שבה רק 24 אחוזים מהציבור הביעו אמון בממשלה, מסר ממשלתי עלול היה להיתפס כהוכחה נוספת לנרטיב שלפיו הממשלה מסתירה מידע.¹²³
2. פיצול אחריות פוגע בעקביות: היעדר הגדרה ברורה של הגורם המוביל פוגע במסר. מחלקת התקשורת האסטרטגית הצ'כית סבלה מחילופי הנהגה תכופים, מימון מוגבל ומנדט בלתי מוגדר, מה שהוביל למסרים לא עקביים ולעיכובים בתגובה.¹²⁴
3. מהירות ההפצה יוצרת פער מבני: תוכן מניפולטיבי מגיע לווראליות תוך דקות, בעוד שבדיקת עובדות ואימות מקור מצריכים זמן. כשההפצה מתפרסמת באיחור היא מגיעה לשבריר מהקהל שנחשף לטענה המקורית.¹²⁵
4. פרדוקס ההגברה: חזרה על מידע כוזב לצורך הפרכתו עלולה להגביר את חשיפתו ולהדהד את הקמפיין. Operation Overload, קמפיין שמטרתו להציף בודקי עובדות ועיתונאים, ניצל פער זה במכוון כדי לאלץ עיתונאים לעסוק בתכנים שלו במקום בתכנים אותנטיים. תגובה אסטרטגית מחייבת תעדוף קפדני ואיפוק מול טענות שתפוצתן נמוכה.¹²⁶
5. קהלים שונים צורכים מידע בפלטפורמות, שפות ומסגרות חברתיות שונות: הודעות ממשלתיות רשמיות אינן מגיעות לצעירים בטיקטוק, למבוגרים המקבלים תוכן בדואר אלקטרוני או לקהילות מיעוטים בערוצי טלגרם סגורים, המחייבים מענה לשוני ותרבותי מותאם.¹²⁷

אוריינות דיגיטלית וחוסן ציבורי

אוריינות דיגיטלית וחוסן חברתי מהווים קו הגנה אזרחי ראשון מפני איומי FIMI. אלה נועדו לחזק את יכולתם של אזרחים לזהות מקור בלתי אמין, להבין כיצד פועלות מניפולציות דיגיטליות, להבחין בין הפצה אורגנית לבין הגברה מתואמת ולהימנע משיתוף תוכן מטעה.¹²⁸ בניגוד להסרת חשבונות או להפרכת טענה נקודתית, מדובר במאמץ מתמשך לחיזוק חוסנה של סביבת המידע.¹²⁹

לקח מרכזי הוא כי אין להתייחס לציבור כאל קבוצה אחידה – הפגיעות למניפולציה משתנה בהתאם לגיל, שפה, מיקום, הרגלי צריכת מידע ורמת אמון במוסדות.¹³⁰ בפולין ובצ'כיה הוגדרו צעירים ובני הגיל השלישי כאוכלוסיות פגיעות: צעירים – בשל צריכת מידע בסביבות אלגוריתמיות, ומבוגרים בשל קושי בזיהוי תוכן סינטי והסתמכות על רשתות תפוצה סגורות.¹³¹ במולדובה תורגמו הפערים למאפייני שפה וזהות: דוברי רוסית, קהילות דתיות, אזרחי המדינה המתגוררים מחוצה לה ואוכלוסיות כפריות נחשפו לנרטיבים ייעודיים בפלטפורמות שונות.¹³² פערים אלו מוכיחים כי אוריינות דיגיטלית מחייבת פילוח קהלים מדויק והתאמה לא רק של השפה והפלטפורמה אלא גם של זהות הדובר (מורה, עיתונאי, משפיען) הנתפס כאמין יותר מול כל קהל יעד.¹³³

יוזמות ממשלתיות

היוזמות הממשלתיות האפקטיביות ביותר לא הסתפקו בסיסמאות כלליות נגד חדשות כזב, והסבירו טקטיקות ספציפיות של מבצעי השפעה: התחזות, שימוש ברגשות, דיג, חשבונות פיקטיביים והסתרת מקור המימון.¹³⁴

בגרמניה הובילו משרד המשפטים וקואליציות אזרחיות פרויקטים להדרכת קהלים מבוגרים, הצפויים לפגיעות רבה לדיסאינפורמציה, והפיצו ערכות כלים לזיהוי רשתות התערבות זרות.¹³⁵ בפולין שולבו פעילויות של אוריינות דיגיטלית שכללו מפגשים, הכשרות לגורמי בחירות ולעיתונאים והפצת חומרי הסברה, וכן הועמדו לרשות הציבור כלים דוגמת סריקת דומיינים והתרעות על פגיעה אפשרית בחשבונות NASK הובילה קמפיין ציבורי שהתמקד באופן שבו דיסאינפורמציה מנצלת רגשות, בפרט פחד וכעס, כדי להשפיע על התנהגות.¹³⁶ בצ'כיה פרסמו משרדי הממשלה מידע לגבי הצבעת הדואר, בטיחות ההליך ותפקיד ה-DSA.¹³⁷

הדוגמה המובהקת והמצליחה בעולם לגישת 'החיסון הקוגניטיבי' המונע היא מדיניות האוריינות הדיגיטלית הלאומית של פינלנד, שנוסחה על ידי משרד החינוך והתרבות הפני בשנת 2019. פינלנד מתייחסת לאוריינות הדיגיטלית של אזרחיה כאל חלק בלתי נפרד מתפיסת הביטחון הלאומי שלה ומגדירה אותה כעמידות מול 'תרחישי איום חברתיים' מוגדרים – הפצה ממוקדת של דיסאינפורמציה ומסרים אנטי-דמוקרטיים מצד רוסיה. המודל הפני מראה כי הגנה על טוהר הבחירות והאמון הציבורי אינה יכולה להישען על קמפיין הסברה נקודתי בסמוך ליום ההצבעה, אלא מחייבת חיסון קוגניטיבי ארוך טווח שיקנה לכלל קבוצות הגיל מיומנויות חשיבה ביקורתית לזיהוי מניפולציות המנסות לפגוע בהליך הדמוקרטי.¹³⁸

יוזמות חברה אזרחית

החברה האזרחית מובילה חלק ניכר מהאוריינות הדיגיטלית, ויתרונה בגמישות וביכולת לפתח תכנים מותאמים לקהלים שונים, וכן לפעול במגוון אמצעים ובאמינות עצמאית שאינה מזוהה עם הממשלה.¹³⁹

בצ'כיה התקיימו פעילויות אוריינות דיגיטלית לבני נוער, סדנאות ייעודיות לאוכלוסיות מבוגרות שנמצאו כצרכניות המרכזיות של שרשראות מיילים ותעמולה, והופקו קורסים דיגיטליים פתוחים ותוכניות הדרכה לעיתונאים מקומיים. במדינה זו הושקו כלי אימות מבוססי AI לזיהוי תעמולה רוסית, וכלי תקשורת וארגוני בדיקת עובדות שילבו בין אימות מידע לבין הסבר על הערכת אמיתות הטענה והמקור. נוסף על כך, סרט תיעודי על אודות אנשים בעלי נטייה לאמונות קונספירטיביות הופץ בסמוך לבחירות כדי לעורר דיון ציבורי בנושא.¹⁴⁰

בפולין השיקה קרן PZU (זרוע הפילנתרופיה של חברת הביטוח הגדולה במדינה) קמפיין מודעות ציבורית רחב שעודד חשיבה ביקורתית ושילב בתי ספר, ידוענים ומשפיענים, מה שאפשר הגעה לקהלים שלא היו נחשפים לקמפיין ממשלתי.¹⁴¹ בגרמניה תרמו הדוחות, ההתרעות והמיפויים של ארגוני המחקר לא רק לניטור אלא גם לחינוך הציבור והתקשורת – הצגת דוגמאות של אתרי מראה, תוכן סינתטי ורשתות מתואמות סייעה להמחיש את ההבדל בין טענה כוזבת יחידה למבצע השפעה.¹⁴²

במולדובה הובילו ארגוני חברה אזרחית קמפיין שטח וסרטונים המותאמים למיעוטים לשוניים, במטרה להעלות את המודעות לשימוש ב-AI ובחשבונות פיקטיביים בתשלום. ארגונים מקומיים ועיתונאים פעלו לקידום מודעות ציבורית, לחשיפת אתרים מתחזים ולהסברת הקשרים בין רשתות מקומיות לתשתיות פרו-רוסיות – פעילות חיונית בקהילות שבהן נרשמה רמת אמון גבוהה במקורות תקשורת רוסיים.¹⁴³

מגבלות האוריינות הדיגיטלית

במסגרת תפיסת ההתמודדות, אוריינות דיגיטלית היא רכיב הכרחי אך לא מספיק. תרומתה תלויה בשילובה עם שאר אמצעי המענה, וחמש מגבלות מבניות מגדירות את גבולותיה:

1. חלק מהפעילות הזרה מתוכנן להיראות אותנטי: אתרי מראה, סרטונים מבוססי AI, התחזות לכלי תקשורת ורשתות של משתמשים מקומיים מקשים גם על משתמשים מיומנים לזהות מניפולציה.¹⁴⁴
2. תוכניות אוריינות אינן מגיעות באופן שווה לכל הקהלים: יוזמות המופעלות בבתי ספר אינן מגיעות לבני הגיל השלישי, קמפיינים ברשתות חברתיות אינם מגיעים לקהילות בקבוצות סגורות ותכנים בשפה הלאומית אינם נותנים מענה למיעוטים לשוניים. ללא התאמה שיטתית, הפעילות נוטה להגיע דווקא לאזרחים שכבר מודעים לבעיה.¹⁴⁵
3. קמפיין קצר לפני הבחירות אינו תחליף לחינוך ארוך טווח: יכולת להעריך מקור ולזהות מניפולציות מחייבת תרגול מתמשך ושילוב במערכת החינוך ובהכשרות עובדי ציבור ועיתונאים.¹⁴⁶
4. הדגשת האחריות האישית עלולה להעביר לאזרחים נטל לא-מידתי: משתמש יחיד אינו יכול לחשוף מי מימן רשת חשבונות, או כיצד תוכן קודם באלגוריתם. מידע זה מצוי בידי המדינה והפלטפורמות, ואוריינות דיגיטלית אינה יכולה לשמש הצדקה להפחתת אחריותם בהתמודדות.
5. פרדוקס החשדנות ושחיקת האמון הממסדי: פיתוח ספקנות הוא יעד מרכזי של האוריינות הדיגיטלית, אך חשיפת יתר לשיטות מניפולציה עלולה לעורר חשדנות וציניות בקרב הבוחרים.¹⁴⁷ במקום לפתח חשיבה ביקורתית, אזרחים עלולים לאבד אמון בכל מקור מידע שהוא, לרבות כלי תקשורת ממסדיים ורשויות מדינה, ובכך תושג מטרת התוקף.¹⁴⁸

מסקנות והמלצות מדיניות לישראל

הניסיון שנצבר בגרמניה, בפולין, בצ'כיה ובמולדובה, לצד המעטפת המוסדית והרגולטורית של האיחוד האירופי, מציע מפת דרכים לפיתוח מענה לאתגר ה-FIMI בישראל.

הצורך בגיבוש מסגרת פעולה מותאמת מקבל משנה תוקף ודחיפות לאור ממצאי דוח מבקר המדינה מיולי 2026. הדוח חשף פערים מערכתיים חמורים בהיערכותה של ישראל לבחירות: אף שאיום ההשפעה הזרה וגיוס השיח הציבורי הוגדרו על ידי גופי המטה והביטחון (המל"ל, שב"כ, מערך הסייבר הלאומי וגורמים נוספים בקהילת הביטחון) כסיכון אסטרטגי כבר בשנת 2017, ישראל עודנה פועלת ללא מדיניות לאומית מאושרת, ללא הגדרת אופרטור מוביל וללא גורם מתכלל קבוע. כתוצאה מכך המענה הישראלי נותר מבוזר, מקוטע ומאופיין בדפוס של יוזמות שלא יצאו לפועל, כאשר עיקר ההיערכות והעיסוק המבצעי מתרחשים באופן תגובתי רק בסמוך למערכת בחירות. המבקר הזהיר כי היעדר מענה מוסדי רציף וקבוע מותיר את הציבור חשוף למניפולציות מידע עיונות, המנצלות שסעים חברתיים וקטוב לאומי כדי לערער את האמון במוסדות הדמוקרטיים – סיכון המגיע לשיאו לקראת הבחירות לכנסת ה-26.¹⁴⁹

בפרק זה נסקרים סביבת המידע הישראלית והפערים בה ולאחר מכן נמנים לקחים, תחילה ברמה המדינתית, באמצעות בחינת עקרונות להתמודדות עם FIMI שנבחנו הלכה למעשה במדינות אירופה, ולאחר מכן ברמת החברה האזרחית.

מרחב המידע הישראלי לקראת בחירות אוקטובר 2026: הפערים

הזירה הדיגיטלית הישראלית בתקופת בחירות מתאפיינת בשיח פוליטי יצרי וסוער, קטוב חברתי עמוק, צריכת חדשות ברשתות חברתיות ובערוצים מוצפנים וסגורים (דוגמת טלגרם ו-ווטסאפ) וגם במבנה דמוגרפי מורכב בעל מגזרים מובחנים (כגון דוברי רוסית, דוברי ערבית, החברה החרדית) המקשים על ניטור וזיהוי קמפיינים.¹⁵⁰ במערכות הבחירות האחרונות (הכנסת ה-21 עד ה-25) זוהו ניסיונות מתמשכים מצד שחקנים זרים, בעיקר איראן ורוסיה, לצד שחקנים מקומיים, להשפיע באופן מניפולטיבי על דעת הקהל.¹⁵¹ ניסיונות אלו כללו הפעלת רשתות של חשבונות פיקטיביים, בוטים, אתרי מראה, התחזות לכלי תקשורת ולגורמים פוליטיים והפצת דיסאינפורמציה ממוקדת, שמטרתה להעמיק את השסעים, לזרוע ייאוש, לשנות את הרכבי הרשימות ולדכא הצבעה בקרב קבוצות אוכלוסייה מובחנות.¹⁵²

מערכת הבחירות לכנסת ה-26 צפויה להתנהל תחת איום של מבצעי FIMI. בעוד דמוקרטיה באירופה פיתחו בשנים האחרונות תפיסות ויכולות תגובה אזרחית-ממשלתית רב-שכבתית, הניתוח המצטבר של זירת המידע הישראלית – כפי שעולה מדוחות המחקר של הכנסת,¹⁵³ מסדרת הסימולציות האסטרטגיות שהתבצעו **במכון למחקרי ביטחון לאומי** מ-2019 ועד 2026¹⁵⁴ ומדוח מבקר המדינה¹⁵⁵ – מלמד כי **ישראל מצויה בעמדת פגיעות קשה**. פגיעות זו אינה נובעת ממחסור בטכנולוגיה או ביכולות מקצועיות אלא מכשל תפיסתי עמוק, פערים מושגיים, וואקום מוסדי ומערכת הגנה מפוצלת.¹⁵⁶

שישה פערים מרכזיים מאפיינים את מרחב המידע הישראלי לקראת בחירות 2026:

- 1. הכשל התפיסתי והפערי המושגי:** בישראל קיים פער מושגי מתמשך בין השפעה זרה לגיטימית לבין התערבות זרה, FIMI, שהיא עוינת, מניפולטיבית, מנוגדת לחוק ולערכים הדמוקרטיים ופוגעת באינטרסים ברמת הביטחון הלאומי.¹⁵⁷ שטוש זה מוקצן עקב התמזגות קמפיינים זרים במניפולציות פוליטיות מקומיות ורתימת משפיענים מקומיים.¹⁵⁸ פער זה, כמו גם חוסר בשפה משותפת לתיג איומים, יוצרים קושי מובנה בהתמודדות אחידה עם האיום.

2. מערכת מפוצלת ואקום מוסדי: כפי שמצא דוח מבקר המדינה, ישראל פועלת ללא מדיניות לאומית מאושרת, ללא אופרטור מוביל וללא גורם מתכלל קבוע, תוך התרכזות ב"כיבוי שריפות" בסמוך לבחירות.¹⁵⁹ מהסימולציות עולה כי בישראל קיימים מרבית הרכיבים ויכולות הניטור הנדרשים להגנה על טוהר הבחירות, אולם הם פועלים במנותק ובמבוזר. הפער המרכזי אינו טכנולוגי, אלא היעדרו של מנגנון אינטגרטיבי שיחבר בין גופי הביטחון, הרגולציה והמגזר האזרחי, לשיתוף ידע ותיאום תגובות בזמן אמת.¹⁶⁰

3. מוכנות טכנולוגית מול פגיעות תודעתיות: בעוד שהמערכות בישראל ערוכות למתקפות סייבר על תשתיות ההצבעה ופנקס הבוחרים, הבחירות והשיח הציבורי אינם מוגדרים כתשתית קריטית ולא קיים עיסוק בתוכן או בהטיית דעת קהל.¹⁶¹ מהסימולציות שנערכו עולה כי המערכות סובלות מעיוורון מול תקיפות קוגניטיביות המכוונות לפגיעה בלגיטימיות של ועדת הבחירות, לשיבוש סקרים ומדגמים ולליבוי הפרות סדר. פער זה מועצם עקב מהירות ההפצה של ידיעות כזב ברשתות, הפועלת בקצב מהיר בהרבה ממעני התגובה הלאומיים.¹⁶²

4. ואקום רגולטורי: בהיעדר מסגרת רגולטורית מחייבת, הכללים ברשתות החברתיות נקבעים על פי תנאי השימוש המסחריים של הפלטפורמות, שהאלגוריתמים שלהן מתגמלים תכנים מעוררי זעם וקטוב. בשל כך ישראל תלויה באופן מוחלט ברצון הטוב ובקצב התגובה האיטי של הפלטפורמות, ללא יכולת אכיפה מול בוטים, פרופילים מזויפים או שימוש לרעה ב-AI.¹⁶³ יתרה מכך, ישראל מתמודדת עם קושי מבצעי חריף בסיכול מניפולציות בערוצים סגורים ומוצפנים, שבהם זיהוי מקור ההתערבות ועצירת ההפצה מורכבים במיוחד.

5. הגבול הדמוקרטי של גופי הביטחון וחשש מתיוג פוליטי: גופי הביטחון במדינה מנועים חוקית וערכית מפיקוח על המרחב האזרחי הגלוי וממתן חוות דעת על לגיטימיות של תכנים פוליטיים פנימיים. מתח מובנה זה מונע הגנה אפקטיבית כשתקיפה זרה מתמזגת בשיח מקומי אותנטי, והוא מעצים את החשש של ארגוני חברה אזרחית מפני שיתוף פעולה עם רשויות המדינה ותיוג פוליטי.¹⁶⁴

6. קיהול (טרגוט) מגזרי מותאם אישית: יריבים זרים עלולים לנצל מאפיינים דמוגרפיים באמצעות קיהול מותאם, במטרה לדכא הצבעה, לערער את אמון הציבור ולנסות להצית אלימות וכאוס. מדובר בחולשה מובנית, בייחוד לקראת בחירות.¹⁶⁵

כל אחד מששת הפערים שנסקרו אינו עומד בפני עצמו, הם מזינים זה את זה ומצטברים לכדי פגיעות מבנית אחת: **היעדר חיבור בין הגורמים המחזיקים בידע וביכולות.** תובנה זו מדגישה כי בניית חוסן לאומי לקראת מערכות בחירות עתידיות מחייבת מעבר מתפיסה מבוזרת, שבה גופים פועלים במקביל ובנפרד, לתפיסה של מערכת משולבת, מתואמת ורציפה. ואולם אינטגרציה בין גופי הביטחון לבדם אינה מספקת.

כפי שמראה עמית אשכנזי, המענה להתערבות זרה במרחב הדיגיטלי אינו יכול להישען על הכלים הביטחוניים-טכנולוגיים בלבד, אלא מחייב גישה הוליסטית המחברת ביניהם לבין "קומה אזרחית" של אסדרה, הטלת חובת ניהול סיכונים על הפלטפורמות הגדולות והקמת מנגנון לפיקוח ולדיאלוג עימן.¹⁶⁶ חשיבותה של קומה אזרחית מתחדדת דווקא לנוכח הכשל הדמוקרטי: משום שגופי הביטחון מנועים מלפעול במרחב האזרחי הגלוי, נדרש גורם אזרחי-אסדרתי שיסגור את הפער. המסגרת הנדרשת היא **ארכיטקטורה לאומית המקשרת בין גופי הביטחון, הרגולטור האזרחי הפלטפורמות והחברה האזרחית** בממשקים מסודרים וקודים משותפים – תשתית שהיא התנאי להתמודדות אפקטיבית ומתמשכת עם השפעה זרה, להבדיל ממענה נקודתי בסמוך למועד הבחירות.

המלצות למדיניות

הניתוח ההשוואתי של ארבעה מקרי הבוחן – ארבע מדינות אירופיות – מציג מנעד רחב של פתרונות מוסדיים, רגולטוריים ואזרחיים להתמודדות עם איומי התערבות זרה ומניפולציה במרחב המידע. מנגד, אבחון זירת המידע הישראלית חשף ואקום אסטרטגי, פיצול מבני, היעדר המשגה לאומית מוסכמת והסתמכות כמעט בלעדית על הגנת סייבר טכנולוגית.¹⁶⁷ כדי לתת מענה לפערים שמופו נדרש מתווה מעשי, המבוסס על מערך פעולה מתואם שמפריד בין זרועות המדינה לחברה האזרחית. להלן חמש המלצות אופרטיביות להתמודדות עם FIMI בשגרה ולקראת מערכות בחירות בפרט, המשלבות את המודלים האירופיים עם הדרישות והאילוצים הייחודיים של המערכת הישראלית:

המלצה 1: מינוי גורם מתאם לאומי קבוע לצד ועדת הבחירות – יש למנות אופרטור לאומי ייעודי קבוע להתמודדות עם FIMI, הפועל ברציפות בשגרה ובחירום. האופרטור יעסוק בגיבוש איום הייחוס, בניין כוח, ניטור רציף, ניהול הממשק מול הפלטפורמות והחברה האזרחית וחקר טקטיקות איום מתפתחות. לצד זאת, ועדת הבחירות תשמור על מנדט ניהול ההליך סביב הבחירות, תוך הסתמכות על תמונת המצב של האופרטור בלי שהיא תהפוך בעצמה לגוף ניטור.¹⁶⁸

המלצה 2: מיסוד ערוצי ניטור ושיתוף פעולה עם החברה האזרחית – יש לקבוע נהלים ברורים לניטור ולאיתות איומי FIMI על בסיס אינדיקטורים התנהגותיים טכניים (למשל חתימות קוד של תוכן סינתטי, רשימות דומיינים מתחזים ודפוסי בוטים), תוך ביסוס ערוצי דיווח רשמיים מול ארגוני חברה אזרחית, אקדמיה ובודקי עובדות.¹⁶⁹ מומלץ לאמץ את מנגנון 'מדווחים' אמין, בהתאם למודל האירופי, המעניק לארגוני החברה האזרחית מעמד מוכר ומתייחס אליהם כאל ערוץ דיווח מועדף מול הפלטפורמות והרגולטור, לצד שימוש במסגרת טקסונומית (דוגמת DISARM) ליצירת שפה טכנית משותפת.

המלצה 3: מיקוד המאמצים הרגולטוריים ברגולציית התנהגות לא אותנטית – כדי להימנע מגלישה לצנזורה פוליטית ופגיעה בחופש הביטוי, על המדינה למקד את מאמצי החקיקה בהפללת דפוסי התנהגות מניפולטיביים ותשתיות טכניות, ולא בבדיקת אמיתות התוכן.¹⁷⁰ כך תפעל המדינה נגד תשתיות האיום על בסיס ראיות טכניות והתנהגותיות בלי שתידרש להכריע מהו מידע לגיטימי. המלצה זו מתבססת על גישת הרגולציה של האיחוד האירופי, המגדירה FIMI על פי התנהגות וטקטיקות ולא לפי צנזור תוכן פוליטי, וכך נמנעת הפיכת המדינה ל"משטרת אמת".

המלצה 4: מעבר מהפרכה בדיעבד להפרכה מטרימה ממוקדת ותקשורת אסטרטגית לפי פילוח דמוגרפי – יש לגבש מדיניות תקשורת פרואקטיבית וממוקדת שמנגישה לציבור מראש את טקטיקות המניפולציה הספציפיות והנרטיבים הצפויים, תוך פילוח דמוגרפי לפי גיל, שפה, פלטפורמה, וזהות הדובר.¹⁷¹ תנאי להצלחה, המבוסס על לקחי הניתוח ההשוואתי, הוא מיקוד – אזהרות כלליות ומפחידות מפני חדשות כזב אינן אפקטיביות, ואף עלולות להגביר חרדה ציבורית ולשמש למניפולציה פוליטית. המלצה זו נשענת גם על המלצת מבקר המדינה להגדרת תוכני אוריינות דיגיטלית כחובה במערכת החינוך ולהרחבת ההסברה הממשלתית המותאמת לקהלי יעד שונים. ממצאי הסימולציות שנערכו במכון למחקרי ביטחון לאומי הדגימו כי הודעות דוברות רשמיות אינן נקלטות בקרב מגזרים ייחודיים, וכי רק גיוס מותאם של דוברים קהילתיים מצליח לבסס בזמן אמת חוסן מפני FIMI.

המלצה 5: עיגון שיתוף הפעולה עם הפלטפורמות – יש להמיר קשרים אישיים ואד הוק עם ענקיות הטכנולוגיה בערוצי עבודה מוסדיים ומחייבים ולהעביר מידע ברמת הרשת – דפוסי פעילות וקבוצות חשבונות מתואמות – ולא להסתפק בדיווח על פרסום יחיד.¹⁷² על ישראל להחיל את הסטנדרטים של ה-DISA ואת קוד ההתנהגות האירופי בנושא דיסאינפורמציה, הדורשים מהפלטפורמות ניהול סיכונים אלקטורליים, שקיפות אלגוריתמית ופתיחת נתונים למחקר. נוסף על כך, מהניתוח ההשוואתי עולה כי פנייה לפלטפורמות לגבי תכנים קונקרטיים נכשלת בשל איטיות התגובה, בעוד העברת מידע תשתיתי על רשתות מאפשרת הסרה רוחבית.

המלצות לחברה האזרחית

ארגוני חברה אזרחית מהווים עוגן חיוני להגנת מרחב המידע בזכות גמישותם המבצעית, היכרותם עם הקשרים מקומיים ואמינותם הציבורית, המאפשרות להם לזהות קמפיינים מניפולטיביים במהירות גבוהה בהרבה מגופי המדינה. עם זאת, כפי שעלה בסימולציות שנערכו במכון למחקרי ביטחון לאומי ובדוח מבקר המדינה, **החברה האזרחית בישראל פועלת כמערכת מפוצלת**, המאופיינת בחשדנות הדדית בינה לבין גופי המדינה ובחשש לתיוג פוליטי חד-צדדי, וכן חסר בה מנגנון אינטגרטיבי לשיתוף מידע בזמן אמת.

כדי לממש את פוטנציאל חיזוקה של החברה האזרחית לקראת הבחירות, מומלץ לאמץ את הצעדים הבאים:

1. הקמת קואליציה אזרחית לאומית להגנה על הבחירות (FIMI-ISAC ישראלי) – הקמת רשת אזרחית מאוחדת ומנוהלת שתאגד את ארגוני הניטור, בודקי העובדות, מכוני המחקר והקליניקות המשפטיות באקדמיה. קואליציה זו תכלול שלושה רכיבים חיוניים: ראשית, מאגר דיגיטלי משותף – אימוץ המודל האירופי ליצירת פלטפורמה מאובטחת לשיתוף אינדיקטורים התנהגותיים בזמן אמת בין השחקנים האזרחיים.¹⁷³ שנית, שפה מקצועית וטקסונומיה אחידה – הגדרת תו תקן מקצועי ואימוץ מסגרת לסיווג איומים, המאפשרת ניתוח אובייקטיבי של CIB ללא גלישה לשיפוט פוליטי של התוכן. שלישית, מינוי "מוביל קהילה" שינהל ויתכלל את המרחב האזרחי למניעת כפילויות, זאת לצד סנכרון מאמצי המחקר וחלוקת עבודה לפי תחומי התמחות ויתרון יחסי.

2. מיסוד מוקד דיווח אזרחי (מוקד 100 בחירות) – כינון מוקד אזרחי לקבלת דיווחים מהציבור הרחב על אודות חשד למניפולציות ברשת, וסיווגם המהיר באמצעות פרוטוקול מוסכם מול הפלטפורמות והמדינה.¹⁷⁴ מודל זה יכלול 'מדווחים אמינים', בדומה למודל האירופי, שבמסגרתו ארגוני הניטור יקבלו מעמד אזרחי מוכר, המבטיח קדימות וערוץ דיווח מועדף וישיר מול צוותי האכיפה של ענקיות הטכנולוגיה. זאת ועוד, בהתאם להמלצת מבקר המדינה, המוקד יכלול ערוץ דיווח רשמי, מאובטח ולא פוליטי בין הקואליציה האזרחית לבין ועדת הבחירות המרכזית, מערך הסייבר הלאומי והשב"כ, להעברת התרעות וממצאים בזמן אמת.

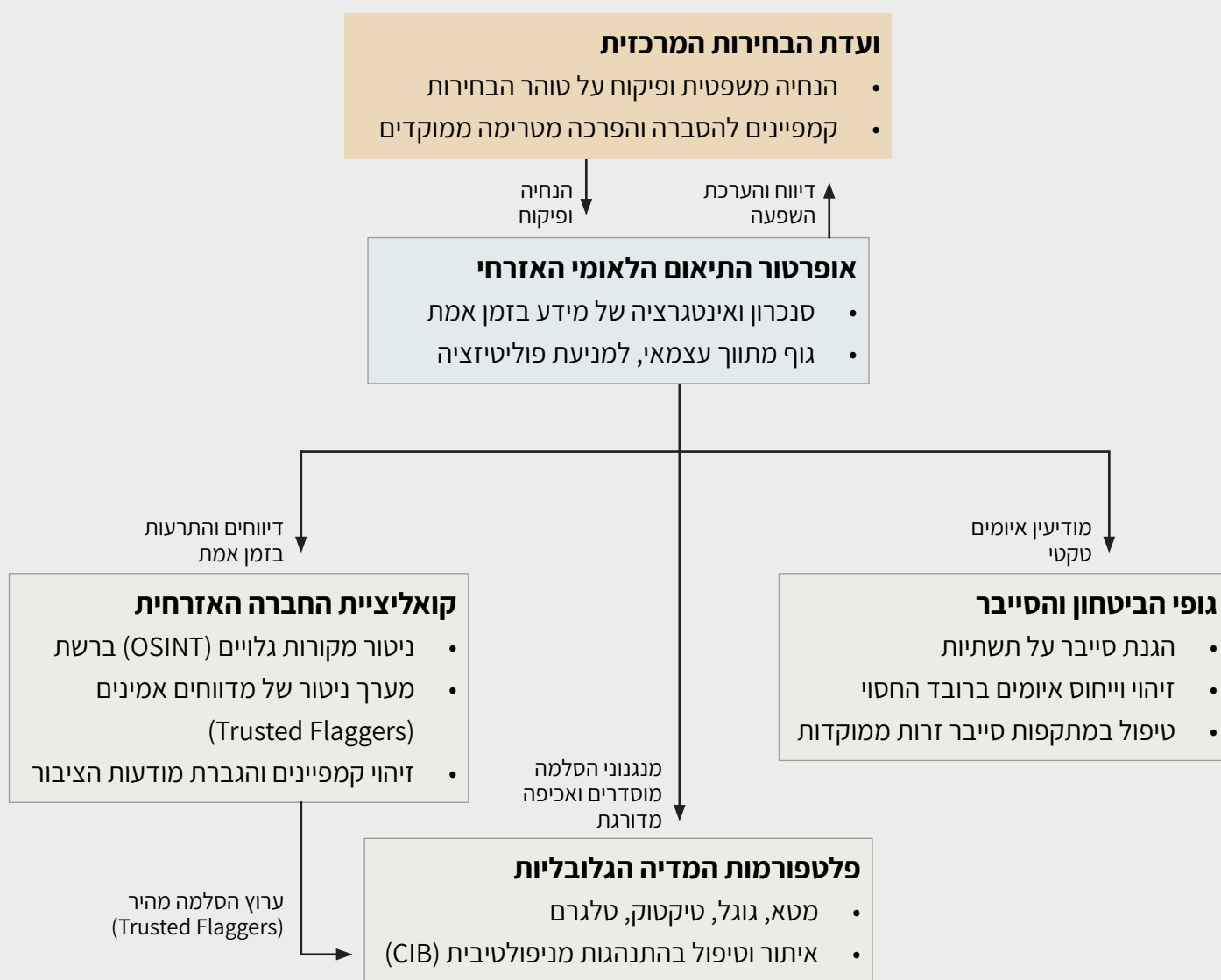
3. שמירה על ניטרליות פוליטית ועצמאות החברה האזרחית – ארגוני חברה אזרחית תורמים באופן מיטבי כשהם נתפסים כעצמאיים מהמדינה ומהשלטון. במדינות שנבחנו מומן חלק ניכר מהפעילות האזרחית, במישרין או בעקיפין, מתקציבים ממשלתיים או מקרנות מחקר לאומיות – תלות שנוצלה על ידי קמפיינים רוסיים כדי להציג את בודקי העובדות כצנזורים מטעם השלטון וכך לשחוק את אמינותם. על הארגונים לבסס מנגנוני שקיפות מלאה לגבי מקורות המימון שלהם ולהפריד בין מקורות המימון ואסדרתם לבין קביעת המדיניות והתוכן. במסגרת זו יש להקפיד על הגדרת פעילות הניטור וההפרכה כעבודה טכנית-התנהגותית בלבד, תוך הימנעות מניסיון לקבוע מהי 'אמת פוליטית', כדי למנוע תיוג פוליטי של החברה האזרחית ולשמור על אמון הציבור.¹⁷⁵

4. פילוח דמוגרפי, אוריינות דיגיטלית וגיוס "נאמני טוהר הבחירות" ומשפיענים קהילתיים – תובנות מהסימולציות שנערכו במכון למחקרי ביטחון לאומי ומהניתוח ההשוואתי מצביעות על צורך לבנות תוכניות להגברת החוסן והאוריינות הדיגיטלית המותאמות למאפיינים הייחודיים של כל קהל יעד, וכן לגיוס מנהיגים קהילתיים להפרכת דיסאינפורמציה בזמן אמת.¹⁷⁶

5. עיגון מימון מדינתי קבוע לתשתיות המחקר האזרחיות בשיטת "אורך זרוע" – בהתאם למודל האירופי, כדי לשמור על רציפות הניטור יש לעבור מתמיכה פרויקטלית קצרת טווח למימון מדינתי-מוסדי קבוע של גופי המחקר האזרחיים. כדי ליישב את המתח בין הצורך בשמירה על עצמאות ואמינות הארגונים, ניתוב תקציבים יכול להתבצע דרך קרנות ציבוריות-אקדמיות עצמאיות או נאמנויות ציבוריות.

6. הגנה על תשתיות ידע ומודלי AI – הרחבת זווית הראייה האזרחית מניטור קמפיינים ברשתות החברתיות סביב הבחירות לסיכול שקט של הרעלת נתונים בשלב מוקדם, והכנת מענה לערעור ודה־לגיטימציה של תוצאות הבחירות. במסגרת ההיערכות יש לנטר תשתיות ידע פתוחות, להקים צוותי מעקב אזרחיים ואקדמיים לזיהוי הרעלת נתונים בערכי ויקיפדיה וכן מנועי חיפוש ומודלי שפה (LLM), לצד מחקר מעמיק על אודות צורות חדשות של האיום.¹⁷⁷

איור 3 - ההמלצות המרכזיות להתמודדות עם התערבות זרה



מחקר מדיניות זה הוקדש לניתוח השוואתי של דרכי ההתמודדות של ארבע מדינות באירופה – פולין, צ'כיה, גרמניה ומולדובה – עם איומי התערבות זרה ומניפולציה במרחב המידע במערכות הבחירות של 2025, ובחן אותן מול נקודות תורפה במרחב המידע והמוכנות המוסדית בישראל לקראת בחירות 2026.

המודלים להתמודדות שגובשו באירופה מלמדים כי FIMI אינו איום נקודתי המוגבל לתקופת הבחירות, אלא איום היברידי תשתיתי הקיים ברציפות, בשגרה ובחירום. יתר על כן, הניסיון הבינלאומי מראה כי המפתח להתמודדות אינו צנזור תכנים פוליטיים אלא מיקוד ברגולציית CIB, בוטים, התחזות ושקיפות מימון ומיסוד ערוצי בקרה קבועים מול הפלטפורמות.

ייחודו של מחקר זה בסינתזה הרוחבית שהתבצעה במסגרתו בין המדינות ששימשו מקרי בוחן כדי למפות דפוסי פעולה וכלים חוצי גבולות, בגיבוש מענה מערכתי תפיסתי רציף במקום מענה נקודתי ובתרגום המענה האירופי לארכיטקטורת חוסן אופרטיבית ושימה עבור ישראל. מסקנות המחקר גם מציעות מענה למתח הדמוקרטי המובנה, שבו גופי הביטחון מנועים מניטור המרחב האזרחי הגלוי מחשש לפגיעה בחופש הביטוי.

עם זאת ובהשוואה למקרי הבוחן האירופיים, ישראל אינה מולדובה – אין לה מחסור ביכולות מדינתיות בסיסיות; היא אינה גרמניה – אין לה מעטפת רגולטורית אירופית ומסגרת DSA מחייבת בעלת כוח מיקוח; ואינה פולין או צ'כיה, הנהנות ממטריית הגנה אזורית רחבה. יתרה מכך, הקיטוב הפוליטי החרף בישראל מעורר חשדנות מובנית עמוקה בין מנגנוני המדינה למגזר האזרחי, בניגוד למודל חוסן לאומי שלם (Whole of Society) באירופה, המבוסס על אמון הדדי.

לפיכך **הניסיון הבינלאומי מספק כלים ועקרונות פעולה, אך לא תבנית ישירה להעתקה**, ויש לתרגם לארכיטקטורת הגנה מותאמת למאפיינים המוסדיים והמשפטיים הייחודיים של ישראל, שתמלא את החלל האסטרטגי שחשף מבקר המדינה. על כן, הארכיטקטורה המוצעת במחקר זה מותאמת אישית לישראל באמצעות ארבעה מנגנונים משלימים: אופרטור לאומי קבוע; קואליציה אזרחית ניטרלית; מיסוד מעמד 'מדווחים אמינים'; ומעבר מגישה תגובתית נקודתית להפרכה מטרימה ולתקשורת מטרימה.

היעד הסופי של מבצעי FIMI אינו לשכנע את הבוחר הישראלי בנרטיב כזה או אחר, ואף לא להביא לניצחונה של מפלגה מסוימת. הניצחון האמיתי של היריב מתרחש ברגע שהציבור מאבד את האמון בעצם קיומה של אמת, ומפתח אדישות או ציניות כלפי ההליך הדמוקרטי עצמו. כשהאזרחים מניחים שהכול מזויף ושתוצאות הבחירות "מכורות", הדמוקרטיה קורסת ללא צורך במאמץ נוסף. לכן, ההגנה על מרחב המידע בשגרה ולקראת מערכות בחירות אינה משימה טכנולוגית או משפטית בלבד, אלא מאבק על תוקף החוזה החברתי הקיים ועל האמון ההדדי בין חלקי החברה למוסדות הרשמיים שעומדים בבסיס ההווה הישראלית כמדינה דמוקרטית.

1. European External Action Service (EEAS), "Beyond Disinformation: What is FIMI?" February 6, 2023.
2. EEAS, "1st EEAS report on foreign information manipulation and interference threats: Towards a framework for networked defense," 2023.
3. EEAS, "Beyond Disinformation"; Michael Tomz and Jessica L.P. Weeks, "Public Opinion and Foreign Electoral Intervention. American," Political Science Review, 114, No. 3 (2020): 856–873.
4. U.S. Department of Justice, "Report on the investigation into Russian interference in the 2016 presidential election: Volume I," Office of Special Counsel, 2019; U.S. Senate Select Committee on Intelligence, "Report on Russian active measures campaigns and interference in the 2016 U.S. election, Volume 2: Russia's use of social media," 2019.
5. EEAS, "1st report"; EEAS, "2nd EEAS report on foreign information manipulation and interference," European Union, January 2024; EEAS, "3rd EEAS report on foreign information manipulation and interference threats," 2025.
6. עופר פרידמן, "המשגת המונחים השפעה זרה והתערבות זרה", מודיעין הלכה ומעשה, 10, (2024): 15-8. EEAS, "Beyond Disinformation"; EEAS, "2nd EEAS report".
7. EEAS, "2nd EEAS report".
8. פרידמן, "המשגת המונחים". EEAS, "1st EEAS report". EEAS, "Beyond Disinformation".
9. EEAS, "2nd EEAS report".
10. שם.
11. Alliance4Europe, FIMI-ISAC, FDEI, "Assessment of foreign information manipulation and interference in the 2025 Polish presidential election," 2025; EEAS, "2nd EEAS report".
12. FIMI-ISAC, FDEI, "Czechia country: Election risk assessment," 2025; FIMI-ISAC, FDEI, "Assessment of foreign information manipulation and interference in the 2025 Moldovan parliamentary election," 2025; Alliance4Europe, FIMI-ISAC, FDEI, "Moldova: Country election risk assessment (CERA)," 2025; FIMI-ISAC, FDEI, "Assessment of foreign information manipulation and interference in the 2025 Czech parliamentary election," 2025; FIMI-ISAC, FDEI, "Assessment of foreign information manipulation and interference (FIMI) in the 2025 German federal election," 2025; FIMI-ISAC, FDEI, "Poland: Country election risk assessment (CERA)," 2025.
13. Alliance4Europe, "Assessment of foreign information," 2025; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Czechia country", 2025; FIMI-ISAC, FDEI, "Assessment of foreign information...German," 2025.
14. משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה במרחב הדיגיטלי: דוח ביקורת מיוחד", 7 ביולי 2026.
15. דוד סימן טוב, ועופר פרידמן, "לא כשל בביצוע – כשל בתפיסה: בעקבות דו"ח מבקר המדינה על ההתמודדות עם התערבות זרה בבחירות", מבט על, גיליון 2167, המכון למחקרי ביטחון לאומי, 12 ביולי 2026.
16. Bundesamt für Verfassungsschutz (BfV), "Illegitimate foreign influence operations targeting the upcoming German federal election," January 2, 2025; FIMI-ISAC, FDEI, "Assessment of foreign information... German," 2025.

17. עמית אשכנזי, "הצעה לקווים מנחים להתמודדות ישראל עם השפעה זרה במרחב הסייבר והרשתות החברתיות", מודיעין הלכה ומעשה, 10, (2024): 219-230; סימן טוב ופרידמן, "לא כשל בביצוע". Alliance4Europe, "Assessment of foreign information," 2025; FIMI-ISAC, FDEI, "Moldova: country election"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Czechia country election... 2025 Moldovan"; FIMI-ISAC, FDEI, "Czechia country election... 2025 Moldovan".
18. מרכז המחקר המידע של הכנסת, "הפצת מידע כוזב ותקיפות סייבר לשם השפעה על הבחירות", אפריל 2019. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Czechia country election"; Tomz & Weeks, "Public Opinion information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Czechia country election"; Tomz & Weeks, "Public Opinion information... 2025 Moldovan".
19. משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה"; סימן טוב ופרידמן, "לא כשל בביצוע"; פרידמן, "המשגת המונחים".
20. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Czechia country election"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
21. מרכז המחקר המידע של הכנסת, "הפצת מידע כוזב באינטרנט ותקיפות סייבר לשם השפעה על בחירות", 11 ביוני 2017; מרכז המחקר המידע של הכנסת, "הפצת מידע כוזב באינטרנט"; משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה".
22. מרכז המחקר המידע של הכנסת, "הפצת מידע כוזב באינטרנט"; משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה"; סימן טוב ופרידמן, "לא כשל בביצוע". Alliance4Europe, FIMI-ISAC, FDEI, "Czechia country election"; FIMI-ISAC, FDEI, "Moldova: country election"; Global Affairs Canada, "G7 Rapid Response Mechanism report: Joint monitoring of 2025 Moldovan parliamentary elections," May 11, 2026.
23. Alliance4Europe, FIMI-ISAC, FDEI, "Moldova: country election"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
24. משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה"; BfV, "Illegitimate foreign influence operations"; EEAS, "Beyond Disinformation".
25. EEAS, "Beyond Disinformation"; EEAS, "2nd EEAS report".
26. EEAS, "Beyond Disinformation"; EEAS, "2nd EEAS report".
27. Tomz & Weeks, "Public Opinion".
28. EEAS, "3rd EEAS report".
29. U.S. Department of Justice, "Report on the investigation"; U.S. Senate Select Committee on Intelligence, "Report on Russian active".
30. Constitutional Court of Romania, "Ruling No. 32/2024 on the annulment of the electoral process for the election of the President of Romania in 2024," December 6, 2024.
31. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
32. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
33. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
34. CeMAS, "Authoritarian strategies online: Analysis and monitoring of digital risks during the German federal election 2025," April 14, 2025.
35. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan".
36. Global Affairs Canada, "G7 Rapid Response"; FIMI-ISAC, FDEI, "Poland country election".
37. ISD, "Coordinated disinformation network uses AI, media impersonation to target German election," February 13, 2025; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".

38. FIMI-ISAC, FDEI, "Czechia country". ; Alliance4Europe, FIMI-ISAC, FDEI, "Moldova: country election"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan" ; ISD, "Coordinated disinformation network"; Pablo Maristany de las Casas and Kevin D. Reyes, "The achilles' heel of EU's media sanctions: Reassessing RT Deutsch access ahead of Germany's 2025 federal election," ISD, February 21, 2025; OSCE Office for Democratic Institutions and Human Rights (ODIHR), "Moldova, parliamentary elections, 28 September 2025: Final report," Organization for Security and Co-operation in Europe, February 18, 2026.
39. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech". FIMI-ISAC, FDEI, "Assessment of foreign information... German,"; FIMI-ISAC, FDEI, "Poland country election".
40. Alliance4Europe, "Assessment of foreign information,"; Global Affairs Canada, "G7 Rapid Response"; FIMI-ISAC, FDEI, "Poland country election".
41. FIMI-ISAC, FDEI, "Czechia country" ; ISD, "Coordinated disinformation network"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
42. CeMAS, "Authoritarian strategies online"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,"; FIMI-ISAC, FDEI, "Poland country election".
43. FIMI-ISAC, FDEI, "Czechia country".
44. Atlantic Council, "Lessons on countering foreign manipulation from Moldova's 2025 elections," December 17, 2025; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; Global Affairs Canada, "G7 Rapid Response".
45. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Poland country election".
46. Alliance4Europe, "Assessment of foreign information,".
47. BfV, "Illegitimate foreign influence operations"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
48. Valentin Châtelet and Victoria Olari, "Paid to post: Russia-linked 'digital army' seeks to undermine Moldovan election", Digital Forensic Research Lab, September 24, 2025; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan".
49. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".
50. Alliance4Europe, FIMI-ISAC, FDEI, "Moldova: country election"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan".
51. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; ISD, Coordinated disinformation Network". " FIMI-ISAC, FDEI, "Poland country election".
52. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
53. BfV, "Illegitimate foreign influence operations"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
54. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"..
55. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Poland country election".
56. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Poland country election".

57. EEAS, "2nd EEAS report".
58. BfV, BfV, "Illegitimate foreign influence operations"; FIMI-ISAC, FDEI, "Assessment of foreign information...German,"; FIMI-ISAC, FDEI, "Poland country election".
59. FIMI-ISAC, FDEI, "Poland country election".
60. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Poland country election".
61. BfV, BfV, "Illegitimate foreign influence operations".
62. OSCE – Office for Democratic Institutions and Human Rights, ODIHR, "Moldova's parliamentary elections were competitive but campaign marred by cyberattacks, illegal funding and disinformation, international observers say," Press Release, September 29, 2025; Moldpres, "STISC reported multiple cyberattack attempts on electoral infrastructure", September 28, 2025.
63. משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה".
64. Secrétariat Général de la Défense et de la Sécurité Nationale, "National strategy for countering foreign information manipulation 2026–2030", Premier Ministre - République Française, 2025; VIGINUM, "Rapport d'activité 2024: Service de vigilance et de protection contre les ingérences numériques étrangères", Secrétariat Général de la Défense et de la Sécurité Nationale, Premier Ministre.
65. FIMI-ISAC, FDEI, "Assessment of foreign information...German,".
66. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan".
67. Alliance4Europe, "Assessment of foreign information FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Assessment of foreign information...German,"; FIMI-ISAC, FDEI, "Poland country election".
68. Atlantic Council, "Lessons on countering foreign manipulation"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Assessment of foreign information...German,".
69. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Poland country election".
70. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".
71. CeMAS, "Authoritarian strategies online"; FIMI-ISAC, FDEI, "Assessment of foreign information...German,".
72. Atlantic Council, "Lessons on countering foreign manipulation"; Châtelet & Olari, "Paid to post".
73. Alliance4Europe, "Assessment of foreign information,".
74. Alliance4Europe, "Assessment of foreign information,"; Atlantic Council, "Lessons on countering foreign manipulation"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan".
75. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Assessment of foreign information...German,".
76. FIMI-ISAC, FDEI, "Poland country election".
77. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Czechia country" .
78. Atlantic Council, "Lessons on countering foreign manipulation"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; European Commission, "Commission services and Moldovan authorities conduct a stress test on potential digital hybrid threats to election integrity ahead of Moldova's parliamentary elections," June 12, 2025; FIMI-ISAC, FDEI, "Assessment of foreign information...German,".
79. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".
80. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Poland country election"; OSCE, "Moldova's

parliamentary elections".

81. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Poland country election".

82. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Poland country election".

83. CeMAS, "Authoritarian strategies online"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".

84. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".

85. Alliance4Europe, "Assessment of foreign information,"; CeMAS, "Authoritarian strategies online"; FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; ISD, "Coordinated disinformation network"; ISD, "The achilles' heel"; FIMI-ISAC, FDEI, "Poland country election".

86. Constitutional Court of Romania, "Ruling No. 32/2024".

87. European Commission, "Guidelines for providers of very large online platforms and very large online search engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065," April 26, 2024.

88. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".

89. שם.

90. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan".

91. European Commission, "Guidelines for providers".

92. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; European Commission, "Guidelines for providers"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".

93. European Commission, "Guidelines for providers"; Daniela Alvarado Rincón, "The DSA alone won't save democracy-but its interplay with the rule of law might," Democracy Reporting International, 2025.

94. Parliament of Singapore, "Foreign Interference (Countermeasures) Act 2021 (Act No. 31 of 2021)", Singapore Statutes Online, 2021.

95. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".

96. OSCE, "Moldova's parliamentary elections".

97. FIMI-ISAC, FDEI, Assessment of foreign information... 2025 Moldovan".

98. Constitutional Court of Romania, "Ruling No. 32/2024".

99. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".

100. משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה"; VIGINUM, "Rapport d'activité 2024."

101. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Poland country election".

102. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".

103. FIMI-ISAC, FDEI, "Assessment of foreign information... German,".

104. Atlantic Council, "Lessons on countering foreign manipulation"; FIMI-ISAC, FDEI, Assessment of foreign information... 2025 Moldovan"; European Commission, "Commission services and Moldovan authorities".

105. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".

106. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
107. FIMI-ISAC, FDEI, "Poland country election".
108. FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".
109. BfV, BfV, "Illegitimate foreign influence operations"..
110. Atlantic Council, "Lessons on countering foreign manipulation"; European Commission, "Commission services and Moldovan authorities'.
111. BfV, BfV, "Illegitimate foreign influence operations"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".
112. FIMI-ISAC, FDEI, Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
113. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".
114. CeMAS., "Authoritarian strategies online"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
115. Moldpres, "STISC reported"; OSCE, "Moldova's parliamentary elections".
116. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, Assessment of foreign information... 2025 Moldovan".
117. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".
118. Alliance4Europe, "Assessment of foreign information,".
119. FIMI-ISAC, FDEI, "Czechia country" .
120. CeMAS, "Authoritarian strategies online"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
121. Atlantic Council, "Lessons on countering foreign manipulation"; Châtelet & Olari, "Paid to post".
122. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, Assessment of foreign information... 2025 Moldovan".
123. FIMI-ISAC, FDEI, "Czechia country" .

124. ש.ד.

125. CeMAS, "Authoritarian strategies online"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
126. Alliance4Europe, "Assessment of foreign information,"; ISD, "Coordinated disinformation network".
127. FIMI-ISAC, FDEI, "Poland country election"; FIMI-ISAC, FDEI, "Czechia country" .
128. FIMI-ISAC, FDEI, "Poland country election".
129. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".
130. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, FDEI, "Poland country election".
131. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Poland country election".
132. Global Affairs Canada, "G7 Rapid Response".
133. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".
134. Alliance4Europe, "Assessment of foreign information,"; DFRLab et al., FIMI-ISAC, FDEI, Assessment of

- foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech"; FIMI-ISAC, FDEI, "Poland country election".
135. FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
136. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Poland country election".
137. FIMI-ISAC, FDEI, "Czechia country" .
138. Ministry of Education and Culture [Finland], "Media literacy in Finland: National media education policy," Publication No. 2019:39.
139. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Moldovan"; FIMI-ISAC, FDEI, "Assessment of foreign information... 2025 Czech".
140. FIMI-ISAC, FDEI, "Czechia country" .
141. FIMI-ISAC, FDEI, "Poland country election".
142. CeMAS, "Authoritarian strategies online"; FIMI-ISAC, FDEI, "Assessment of foreign information... German,".
143. Atlantic Council, "Lessons on countering foreign manipulation"; Châtelet & Olari, "Paid to post"; European Commission, "Commission services and Moldovan authorities".
144. CeMAS, "Authoritarian strategies online"; ISD, "Coordinated disinformation network".
145. Global Affairs Canada, "G7 Rapid Response"; FIMI-ISAC, FDEI, "Poland country election".
146. Alliance4Europe, "Assessment of foreign information,"; FIMI-ISAC, FDEI, "Czechia country" .
147. FIMI-ISAC, FDEI, "Czechia country" ; FIMI-ISAC, "ההתמודדות הלאומית עם השפעה זרה"; FDEI, "Assessment of foreign information... 2025 Moldovan".
148. FIMI-ISAC, FDEI, "Czechia country" ; Tomz & Weeks, "Public Opinion".
149. משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה".
150. המכון למחקרי ביטחון לאומי (INSS) ואיגוד האינטרנט הישראלי, "התערבות זרה בבחירות – הממד הדיגיטלי: סיכום סימולציה [מכתב ליו"ר ועדת הבחירות המרכזית ולראשי מערכת הביטחון]", 2 באוקטובר, 2022; משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה".
151. משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה". ענבל אורפז ענבל ודוד סימן טוב, "התערבות זרה והשפעה איראנית ברשתות החברתיות בישראל", פרסום מיוחד, המכון למחקרי ביטחון לאומי (INSS), 10 ביוני 2024.
152. המכון למחקרי ביטחון לאומי, "התערבות זרה בבחירות"; המכון למחקרי ביטחון לאומי, "סיכום סימולציה היערכות לתרחישי איום על הבחירות במרחב הדיגיטלי" [מסמך פנימי שלא פורסם], בשיתוף המכון הישראלי לדמוקרטיה ואיגוד האינטרנט הישראלי, 2021; משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה".
153. מרכז המחקר המידע של הכנסת, "הפצת מידע כוזב באינטרנט"; מרכז המחקר המידע של הכנסת, "הפצת מידע כוזב באינטרנט".
154. המכון למחקרי ביטחון לאומי, "התערבות זרה בבחירות"; המכון למחקרי ביטחון לאומי, "סיכום דיון סימולציה: השפעה בלתי לגיטימית על השיח הציבורי והפוליטי באמצעים דיגיטליים לקראת בחירות 2019 בישראל" [מכתב ליו"ר ועדת הבחירות המרכזית השופט חנן מלצר], המכון למחקרי ביטחון לאומי (INSS), המכון הישראלי לדמוקרטיה ואיגוד האינטרנט הישראלי, 25 בפברואר 2019; המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית להגנה על הבחירות בישראל מפני התערבות זרה ודיסאינפורמציה" [מסמך פנימי שלא פורסם], המכון למחקרי ביטחון לאומי (INSS), 2026; המכון למחקרי ביטחון לאומי, סיכום סימולציה היערכות לתרחישי איום על הבחירות".
155. משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה".
156. סימן טוב ופרידמן, "לא כשל בביצוע".
157. סימן טוב ופרידמן, "לא כשל בביצוע"; פרידמן, "המשגת המונחים".

158. פרידמן, "המשגת המונחים".
159. משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה"; סימן טוב ופרידמן, "לא כשל בביצוע".
160. המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית"; המכון למחקרי ביטחון לאומי, "סיכום סימולציית היערכות לתרחישי איום על הבחירות"; המכון למחקרי ביטחון לאומי, "השפעה בלתי לגיטימית על השיח הציבורי והפוליטי".
161. מרכז המחקר המידע של הכנסת, "הפצת מידע כוזב באינטרנט"; מרכז המחקר המידע של הכנסת, "הפצת מידע כוזב באינטרנט".
162. המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית"; המכון למחקרי ביטחון לאומי, "סיכום סימולציית היערכות לתרחישי איום על הבחירות"; המכון למחקרי ביטחון לאומי, "התערבות זרה בבחירות"; המכון למחקרי ביטחון לאומי, "השפעה בלתי לגיטימית על השיח הציבורי והפוליטי".
163. אשכנזי, "הצעה לקווים מנחים להתמודדות".
164. המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית"; סימן טוב ופרידמן, "לא כשל בביצוע".
165. מרכז המחקר המידע של הכנסת, "הפצת מידע כוזב באינטרנט"; המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית"; המכון למחקרי ביטחון לאומי, "התערבות זרה בבחירות".
166. אשכנזי, "הצעה לקווים מנחים להתמודדות".
167. אשכנזי, "הצעה לקווים מנחים להתמודדות"; משרד מבקר המדינה, "ההתמודדות הלאומית עם השפעה זרה"; סימן טוב ופרידמן, "לא כשל בביצוע".
168. אשכנזי, "הצעה לקווים מנחים להתמודדות"; סימן טוב ופרידמן, "לא כשל בביצוע".
169. אשכנזי, "הצעה לקווים מנחים להתמודדות"; המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית".
170. אשכנזי, "הצעה לקווים מנחים להתמודדות"; פרידמן, "המשגת המונחים".
171. המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית".
172. אשכנזי, "הצעה לקווים מנחים להתמודדות".
173. המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית".
174. המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית"; המכון למחקרי ביטחון לאומי, "התערבות זרה בבחירות".
175. אשכנזי, "הצעה לקווים מנחים להתמודדות"; המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית"; המכון למחקרי ביטחון לאומי, "השפעה בלתי לגיטימית על השיח הציבורי והפוליטי"; משרד מבקר המדינה, 2026.
176. מרכז המחקר המידע של הכנסת, "הפצת מידע כוזב באינטרנט"; המכון למחקרי ביטחון לאומי, "התערבות זרה בבחירות"; המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית".
177. סימן טוב ופרידמן, "לא כשל בביצוע"; המכון למחקרי ביטחון לאומי, "סיכום סימולציה: חברה אזרחית"; המכון למחקרי ביטחון לאומי, "סיכום סימולציית היערכות לתרחישי איום על הבחירות".

אורפז, ענבל וסימן טוב, דוד. "התערבות זרה והשפעה איראנית ברשתות החברתיות בישראל". פרסום מיוחד, המכון למחקרי ביטחון לאומי (INSS) והמכון לחקר המתודולוגיה של המודיעין במרכז למורשת המודיעין, 10 ביוני 2024. <https://tinyurl.com/4xektz7m>

אשכנזי, עמית. "הצעה לקווים מנחים להתמודדות ישראל עם השפעה זרה במרחב הסייבר והרשתות החברתיות". **מודיעין הלכה ומעשה**, 10 (2024): 230-219.

המכון למחקרי ביטחון לאומי. "סיכום דיון סימולציה: השפעה בלתי לגיטימית על השיח הציבורי והפוליטי באמצעים דיגיטליים לקראת בחירות 2019 בישראל" [מכתב ליו"ר ועדת הבחירות המרכזית השופט חנן מלצר]. המכון למחקרי ביטחון לאומי (INSS), המכון הישראלי לדמוקרטיה ואיגוד האינטרנט הישראלי, 25 בפברואר 2019.

המכון למחקרי ביטחון לאומי. "סיכום סימולציית היערכות לתרחישי איום על הבחירות במרחב הדיגיטלי" [מסמך פנימי שלא פורסם]. בשיתוף המכון הישראלי לדמוקרטיה ואיגוד האינטרנט הישראלי, 2021.

המכון למחקרי ביטחון לאומי. "התערבות זרה בבחירות – הממד הדיגיטלי: סיכום סימולציה" [מכתב ליו"ר ועדת הבחירות המרכזית ולראשי מערכת הביטחון]. המכון למחקרי ביטחון לאומי (INSS) ואיגוד האינטרנט הישראלי, 2 באוקטובר 2022.

המכון למחקרי ביטחון לאומי. "סיכום סימולציה: חברה אזרחית להגנה על הבחירות בישראל מפני התערבות זרה ודיסאינפורמציה" [מסמך פנימי שלא פורסם]. המכון למחקרי ביטחון לאומי, 2026.

מרכז המחקר והמידע של הכנסת. "הפצת מידע כוזב באינטרנט ותקיפות סייבר לשם השפעה על מערכות בחירות", 11 ביוני 2017. <https://tinyurl.com/3fxeahe5>

מרכז המחקר והמידע של הכנסת. "הפצת מידע כוזב באינטרנט ותקיפות סייבר לשם השפעה על מערכות בחירות", אפריל 2019. <https://tinyurl.com/bdda887b>

משרד מבקר המדינה. "ההתמודדות הלאומית עם השפעה זרה במרחב הדיגיטלי: דוח ביקורת מיוחד" 7 ביולי 2026. <https://tinyurl.com/2v4kn8r5>

סימן טוב, דוד ופרידמן, עופר. "לא כשל בביצוע – כשל בתפיסה: בעקבות דו"ח מבקר המדינה על ההתמודדות עם התערבות זרה בבחירות". מבט על, גיליון 2167, המכון למחקרי ביטחון לאומי, 12 ביולי 2026. <https://tinyurl.com/37damxfz>

פרידמן, עופר. "המשגת המונחים השפעה זרה והתערבות זרה". **מודיעין הלכה ומעשה**, 10 (2024): 15-8.

Alliance4Europe, FIMI-ISAC, FDEI. "Assessment of foreign information manipulation and interference in the 2025 Polish presidential election." 2025. <https://tinyurl.com/mpjxxmhu>

Alliance4Europe, FIMI-ISAC, FDEI. "Moldova: Country election risk assessment (CERA)." 2025. <https://tinyurl.com/yra3cz9k>

Alvarado Rincón, Daniela. The DSA alone won't save democracy - but its interplay with the rule of law might. Democracy Reporting International. 2025. <https://tinyurl.com/5dr8rvbz>

Atlantic Council. "Lessons on countering foreign manipulation from Moldova's 2025 elections." December 17, 2025. <https://tinyurl.com/2hf5nmef>

Bundesamt für Verfassungsschutz. "Illegitimate foreign influence operations targeting the upcoming German federal election." January 2, 2025. <https://tinyurl.com/5y4u2jhp>

CeMAS- Center for Monitoring, Analysis, and Strategy. "Authoritarian strategies online: Analysis and monitoring of digital risks during the German federal election 2025." April 14, 2025. <https://tinyurl.com/zt3x2c26>

Châtelet, Valentin, & Olari, Victoria. "Paid to post: Russia-linked "digital army" seeks to undermine Moldovan election." Digital Forensic Research Lab, September 24, 2025. <https://tinyurl.com/nhjmdkde>

Constitutional Court of Romania. "Ruling No. 32/2024 on the annulment of the electoral process for the election of the President of Romania in 2024." December 6, 2024. <https://tinyurl.com/mr483kww>

EEAS - European External Action Service. "Beyond disinformation: What is FIMI?" February 6, 2023. <https://tinyurl.com/dwmw2a5k>

EEAS - European External Action Service. "1st EEAS report on foreign information manipulation and interference threats: Towards a framework for networked defense." February 2023. <https://tinyurl.com/2hhnr2pa>

EEAS - European External Action Service. "2nd EEAS report on foreign information manipulation and interference." January 2024. <https://tinyurl.com/ypbef3ky>

EEAS - European External Action Service. "3rd EEAS report on foreign information manipulation and interference threats." March 2025. <https://tinyurl.com/3w9fpf9b>

European Commission. "Guidelines for providers of very large online platforms and very large online search engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065." April 26, 2024. <https://tinyurl.com/ycxj9w76>

European Commission. "Commission services and Moldovan authorities conduct a stress test on potential digital hybrid threats to election integrity ahead of elections." (June 12, 2025). <https://tinyurl.com/4w58e7tz>

FIMI-ISAC, FDEI. "Assessment of foreign information manipulation and interference in the 2025 Czech parliamentary election." 2025a. <https://tinyurl.com/4723wy9h>

FIMI-ISAC, FDEI. "Assessment of foreign information manipulation and interference (FIMI) in the 2025 German federal election." 2025b. <https://tinyurl.com/2xytk7bk>

FIMI-ISAC, FDEI. "Assessment of foreign information manipulation and interference in the 2025 Moldovan parliamentary election." 2025c. <https://tinyurl.com/238zc73s>

FIMI-ISAC, FDEI. "Czechia: country election risk assessment." 2025d. <https://tinyurl.com/y6vf3z2t>

Global Affairs Canada. "G7 Rapid Response Mechanism report: Joint monitoring of 2025 Moldovan parliamentary elections." May 11, 2026. <https://tinyurl.com/5n7b3d5z>

ISD - Institute for Strategic Dialogue. "Coordinated disinformation network uses AI, media impersonation to target German election." February 13, 2025. <https://tinyurl.com/mrxfn4mv>

Margas, Kinga, Nazari, Saman, Wójtowicz, Aleksandra, Andre, Virginie, Sacilotto, Sophie, & Altaeb, Malak. Poland: Country election risk assessment (CERA). FIMI-ISAC. 2025. <https://tinyurl.com/4dh257kn>

Maristany de las Casas, Pablo, and Reyes, Kevin D. "The Achilles' heel of EU's media sanctions: Reassessing RT Deutsch access ahead of Germany's 2025 federal election." ISD - Institute for Strategic Dialogue. February 21, 2025. <https://tinyurl.com/45j8x7ed>

Ministry of Education and Culture [Finland]. "Media literacy in Finland: National media education policy." Publication No. 2019:39. <https://tinyurl.com/3evuh6f9>

Moldpres. "STISC reported multiple cyberattack attempts on electoral infrastructure." September 28, 2025. <https://tinyurl.com/3hw5vh3a>

OSCE Office for Democratic Institutions and Human Rights. "Moldova's parliamentary elections were competitive but campaign marred by cyberattacks, illegal funding and disinformation, international observers say." Press Release. September 29, 2025. <https://tinyurl.com/4p7zth6h>

OSCE Office for Democratic Institutions and Human Rights. "Republic of Moldova: Parliamentary elections, 28 September 2025: Final report." February 18, 2026. <https://tinyurl.com/yc3k23tw>

Republic of Singapore. “Foreign Interference (Countermeasures) Act 2021 (Act No. 31 of 2021).” Singapore Statutes Online. 2021. <https://tinyurl.com/y45ns9xt>

Secrétariat Général de la Défense et de la Sécurité Nationale. National strategy for countering foreign information manipulation 2026–2030. Premier Ministre - République Française. 2025. <https://tinyurl.com/26ex2k6t>

Tomz, Michael ,& Weeks, Jessica. L.P. “Public Opinion and Foreign Electoral Intervention.” American Political Science Review, 114, no. 3 (2020): 856–873. <https://doi.org/10.1017/S0003055420000064>

U.S. Department of Justice. “Report on the investigation into Russian interference in the 2016 presidential election: Volume I of II.” Office of Special Counsel. 2019. <https://tinyurl.com/2w78ha3t>

U.S. Senate Select Committee on Intelligence. “Report on Russian active measures campaigns and interference in the 2016 U.S. election, Volume 2: Russia’s use of social media.” 2019. <https://tinyurl.com/yw75dney>

VIGINUM. “Rapport d’activité 2024: Service de vigilance et de protection contre les ingérences numériques étrangères.” Secrétariat Général de la Défense et de la Sécurité Nationale, Premier Ministre. 2025. <https://tinyurl.com/4ycc7nba>



המכון למחקרי ביטחון לאומי

THE INSTITUTE FOR NATIONAL SECURITY STUDIES



אוניברסיטת תל אביב
TEL AVIV UNIVERSITY