להפעיל עדכוני אבטחה דחופים לתוכנות שברשותם. כדי שההודעות ייראו אמינות, הן אף כללו מידע אמיתי בנוגע לציוד שבשימוש הארגון המותקף. הנוזקה המצורפת להודעות אספה מידע על המערכות המותקפות בטרם השתמשה בתוכנת wiper כדי למחוק את כל מערכת המידע של הארגון. לתקיפה קדמה בחינה מדוקדקת של העובדים הטכניים בכל אחד מן הארגונים המותקפים כדי לגרום נזק מרבי.[192]

תקיפות CNE (ריגול) – עשרות חשבונות איראניים מזויפים במדיה החברתית, בפרט בטלגרם, ניסו לספק לחמאס מודיעין שימושי. בחלק מן המקרים הביעו הפרופילים המזויפים עניין בקשר רומנטי עם חיילי צה"ל כדי לפתותם לחשוף מידע על יחידותיהם ועל המבצעים שהיו מעורבים בהם. פניות נשלחו לאלפי חיילי צה"ל.[193]

תקיפות CNI (תודעה) – איראן הפיצה במדיה חברתית מידע רגשי טעון, מוטה ולעיתים אף שקרי לחלוטין כדי לקעקע את מעמדה של ישראל ולהטיל על ארצות הברית את האשמה בפשעי המלחמה שישראל ביצעה לכאורה. בדרך זו הגיעה איראן לקהל בינלאומי עצום בגודלו וסייעה לחמאס. חשבונות איראניים בפייסבוק ובטוויטר היללו את מעשי הטבח של חמאס נגד אזרחים ישראלים ועודדו התקפות נוספות נגדם.[194]

מבצעי ההסתה והדיסאינפורמציה נגד המתנגדים "למהפכה המשפטית", שהחלו עוד בטרם המלחמה, נמשכו בשבועותיה הראשונים. חשבונות פייסבוק, טוויטר, וואטסאפ, אינסטגרם וטלגרם שימשו לליבוי ולהעצמה של המתחים בחברה הישראלית בנוגע לסוגיות נפיצות, ובכלל זה מעמד ערביי ישראל ועמדות המזוהות עם הימין הישראלי הקיצוני.[195]

192 Israel National Cyber Directorate, "A New Fishing Attack from Iran Tries to Erase Information in Organizations," December 26, 2023, https://www.gov.il/he/departments/news/iranf5_2612.

193 Raphael Kahan, Ynet November 9, 2023

194 Steven Lee Myers and Sheera Frenkel, "In a Worldwide War of Words, Russia, China and Iran Back Hamas," *New York Times*, November 3, 2023, https://www.nytimes.com/2023/11/03/technology/israel-hamas-information-war.html.

195 Raphaela Goichman, "The Iranian Cyber Attacks – More Sophisticated and Destructive," *The Marker*, November 6, 2023, https://www.themarker.com/captain-internet/2023-11-06/ty-article/premium/0000018b-a44b-dc41-af9f-ef6bdcca0000.

חלק 5

מסקנות והמלצות

ההפגנות נגד המשטר ב־2009 ותקיפת הסטקסנט ב־2010 עוררו את העניין של איראן בתחום הסייבר, ומאז השתפרו יכולות הסייבר שלה במידה ניכרת. בעשור האחרון הפכה איראן לאחת המדינות הפעילות ביותר בלוחמת סייבר, והיא כנראה נמנית עם מובילות המעגל השני של השחקניות הגלובליות, או קרוב לכך. הכמות והתחכום של התקיפות שאיראן ניהלה גדלו, והיא הוכיחה יכולת להרוס, לשבש, לעוות, לחבל ולערער תשתיות לאומיות חיוניות, אינטרסים מסחריים, יכולות צבאיות, פוליטיקה פנימית, חוסן חברתי ודיפלומטיה בינלאומית. יכולותיה של איראן ימשיכו ככל הנראה להשתפר על בסיס יכולותיה שלה ובעקבות סיוע רוסי וסיני.

סביר להניח שאיראן סיפקה לחזבאללה יכולות סייבר מתקדמות, בדיוק כפי שעשתה בתחומים אחרים, אך הראיות הזמינות אינן מספיקות כדי לבסס מסקנה זו במלואה. קרוב לוודאי שהחוסר בראיות משקף את מגבלות המידע ולא את מגבלות יכולותיו של חזבאללה. על הג׳האד האסלאמי הפלסטיני יש מעט מידע; במקרה זה ייתכן שמיעוט המידע משקף את המציאות.

בלי לגרוע ולו במעט מעומק האיבה האיראנית כלפי ארצות הברית, ערב הסעודית ומעל לכול כלפי ישראל, חשוב להבין שרבות מפעולותיה של איראן בתחום הסייבר, כמו בתחומים אחרים, נושאות אופי תגובתי והגנתי. לשם המחשה, הפיתוח המהיר של יכולות הסייבר של איראן היה במידה רבה תגובה לתקיפת הסטקסנט, וכך היו גם תקיפת ״אבאביל״ נגד מוסדות פיננסיים אמריקניים והתקיפה נגד חברת ״ארמקו״ הסעודית. איראן הכינה והוציאה לפועל תקיפות סייבר לפני החתימה על הסכם הגרעין ב־2015 ואחריה, הגיבה באמצעי סייבר לחיסולו של מפקד כוח קודס של משמרות המהפכה קאסם סולימאני בידי כוחות אמריקניים, ועל פי דיווחים מנהלת בשנים האחרונות עם ישראל מערכת מתמשכת של מהלומות סייבר הדדיות, ובכלל זה התקיפות על מערכת המים של ישראל ועל נמל התעופה בן־גוריון.

לוחמה אסימטרית הפכה זה מכבר למרכיב חיוני באסטרטגיית הביטחון הלאומי של איראן, והיא נועדה לקזז את יתרונותיהן של יריבותיה החזקות. בניגוד ליריבי העבר של ישראל בעולם הערבי, איראן אינה מחפשת להביס את ישראל בטווח הקרוב משום שהיא

יודעת שאין ביכולתה להשיג מטרה זו. במקום זאת אימצה איראן אסטרטגיית התשה ארוכת טווח שנועדה לחבל בכוחה הצבאי של ישראל, לשחוק את מעמדה הבינלאומי ולערער את חוסנה החברתי כדי להוביל בסופו של דבר לקריסתה. עם השנים גברה חשיבותו של מרכיב הסייבר באסטרטגיית ההתשה הזאת, באסטרטגיית הביטחון הלאומי הכוללת של איראן ובכלים המדיניים שלה. הסייבר אף הולם מאוד את התרבות האסטרטגית של איראן ואת החשיבות הרבה שהיא מייחסת לעמימות, ליכולת הכחשה ולשימוש בשלוחים.

פעולות הסייבר של איראן התרחבו והפכו לגלובליות. היא תקפה מטרות בישראל, בארצות הברית ובערב הסעודית, וגם במדינות אחרות ברחבי העולם. עם הרשימה החלקית של המדינות שהיא תקפה נמנות צרפת, בריטניה, גרמניה, דנמרק, אלבניה, קנדה, אוסטרליה, ניו זילנד, הודו, יפן, בחריין, ירדן, עיראק, טורקיה ואפילו שתי בעלות בריתה החשובות ביותר – רוסיה וסין. סוגי המטרות שהיא תקפה מגוונים לא פחות: פרלמנטים; משרדי ממשלה, לרבות משרדי הגנה ומשרדי חוץ; ספקים בתחום הביטחון; מטרות צבאיות; משלחות דיפלומטיות; חברות תשתית חיונית, לרבות חשמל, מים ותקשורת, בקרת תעבורה אווירית, נפט וגז, בתי זיקוק וצינורות; מוסדות פיננסיים; ארגוני בריאות; חברות תעופה; חברות הייטק וייצור; ארגוני תקשורת; מוסדות אקדמיים; צוותי חשיבה; ארגונים לא ממשלתיים ועוד.

למרות היקף הפעילות של איראן בסייבר, היא עדיין רואה בו אמצעי משלים בלבד ולא אמצעי בפני עצמו. ככזה הוא נועד לתמוך ביכולות הדיפלומטיות, הכלכליות והצבאיות של איראן ולחזק את ההרתעה שלה. הסייבר נחשב גם אמצעי להגברה ולהעצמה של היכולות האסימטריות המסורתיות יותר של איראן, כגון טרור, שימוש בשלוחים ומבצעי תודעה בכלים מסורתיים. הסייבר הוא מכשיר חשוב במיוחד ללוחמה אסימטרית בעבור איראן מכיוון שיריבותיה המובילות, ובהן ארצות הברית וישראל, תלויות בסייבר הרבה יותר ממנה ולכן פגיעות יותר לתקיפה.

כמו מדינות אחרות, כגון ארצות הברית ובריטניה, גם איראן אימצה דוקטרינה צבאית גמישה ורחבת טווח. פירוש הדבר שהיא שומרת לעצמה את הזכות לנקוט הן פעולות התקפיות והן פעולות הגנתיות, בכל אמצעי שתמצא לנכון – קינטי, סייבר או שילוב שכיח יותר ויותר של תקיפות CNE, CNA ו־CNI.

דרך הפעולה של איראן מוכיחה בבירור שהיא לא אימצה מדיניות של "אי־שימוש ראשון" (no first use) בתחום הסייבר. לעומת זאת, אין כל סימן המעיד שאיראן שילבה בין אסטרטגיית הסייבר לאסטרטגיית הגרעין שלה – לא ברור אם היא רואה בתקיפות סייבר

מערכתיות מדרגת הסלמה הנמוכה מן הרמה הגרעינית, ואם שתי צורות התקיפה הן חלק מאסטרטגיית ביטחון לאומי אחת כוללת.

להלן סיכום הממצאים העיקריים של המחקר הנוגעים לתקיפות האיראניות מסוג CNE,CNA ו־CNI ולתקיפות משולבות, לעיתים גם עם תקיפות כופרה.

תקיפות CNA (שיבוש והרס). התקיפות "אבאביל" ו"שאמון" והתקיפות נגד אלבניה, בין השאר, הוכיחו את יכולתה של איראן לגרום לשיבוש כלכלי ניכר. התקיפות האיראניות נגד תשתיות לאומיות חיוניות בישראל, בארצות הברית ובאירופה עדיין לא גרמו להרס חמור, אך הוכיחו שיש בכוחן לעשות זאת. המודיעין האמריקני סבור כי איראן מסוגלת כיום לגרום לנזק, והתקיפות נגד מערכות אספקת המים ובקרת התעבורה האווירית של ישראל הוכיחו שיש בכוחן לגרום לנזק קטלני.

רוב תקיפות ה־CNA שאיראן הוציאה לפועל עד היום לא היו מתוחכמות, וההגנות של שחקניות הסייבר המתקדמות הספיקו בדרך כלל כדי למנוע נזק רב. רוב התקיפות היו נגד יעדים של המגזר הציבורי והפרטי שאינם מוגנים היטב, ובכך העניקו תוקף, לפחות חלקית, לטענה שההגנה על רוב המטרות הישראליות והמערביות החשובות תצליח להתמודד עם מרבית התקיפות פרט למתוחכמות ביותר. עם זאת, השחתות לא מתוחכמות ושיבושים של אתרי אינטרנט מסחריים וממשלתיים שביצעה איראן הצליחו לגרום לאי־נוחות לא מבוטלת ולהשפיע פסיכולוגית על הציבור או על אמון הצרכנים.

המידע הזמין אינו מספיק כדי להעריך במלואה את יכולתה של איראן לערוך מבצעי סייבר צבאיים אפקטיביים ומתמשכים, בניגוד לתקיפות על מטרות אזרחיות ומסחריות המוגנות פחות. מסיבות ברורות המדינות המותקפות וגם איראן עצמה נמנעות מלחשוף את יכולות הסייבר הצבאיות שלהן או פרטים על תקיפות סייבר צבאיות שהופעלו נגדן. איראן גם עדיין לא הראתה יכולות סייבר ברמה לאומית מערכתית. עם זאת, ייתכן שהיא שומרת את היכולות המתקדמות ביותר שלה לנסיבות "המתאימות". ברי שתחום הסייבר אכן מספק לאיראן ולבעלות בריתה ארגז כלים חשוב, שבאמצעותו היא יכולה לנהל מתחת לרדאר מבצעים שניתנים להכחשה.

תקיפות CNE (ריגול). עצם אופיו החשאי של עולם הריגול מקשה להעריך במלואה את האפקטיביות של תקיפות ה־CNE שאיראן ביצעה עד כה. לכל הפחות הן היו רבות והשיגו מידה מסוימת של מידע מסווג בעל משמעות. תקיפות CNE נועדו להשיג כמה מטרות. חלקן נועדו לאסוף מידע מודיעיני על תעשיות ביטחוניות, על תוכניות לפיתוח נשק, על יכולות

צבאיות כוללות, על מדיניות הגרעין של ישראל ועל החשיבה המדינית והאסטרטגית של ארצות הברית, ישראל והמערב. אחרות נועדו לסייע בהכנה של תקיפות CNA ו־CNI עתידיות, לרבות נגד חברות ביטחוניות, או כדי להשיג תובנות על היכולות המדעיות והטכנולוגיות של ישראל ומדינות אחרות. מבצעי CNE לגיוס מחבלים ולהכנה לפיגועי טרור הם איום גובר.

היתרון המודיעיני שאיראן וגורמים אחרים הרוויחו לכאורה מן התקיפות על החברות "שירביט" ו"KLS מימון רכב" הוא המקבילה הישראלית לנזק שנגרם לארצות הברית מן התקיפה הרוסית הידועה לשמצה על חברת SolarWinds (שגם ישראל הייתה קורבן משני שלה). המחדל המודיעיני שנחשף בתקיפות נגד "שירביט" ו־KLS הועצם באמצעות קמפיין התודעה האיראני שבוצע לאחריהן והפיץ את המידע הגנוב באינטרנט כדי לפגוע במוניטין של ישראל.

השימוש של איראן בתקיפות CNE למעקב אחר מתנגדי משטר באיראן ומחוצה לה ולדיכויים הוא, על פי דיווחים, אפקטיבי במיוחד. השליטה של איראן בעולם הסייבר באמצעות רשת NIW ובאמצעות מגוון כלי סייבר אחרים משמשת את המשטר כדי לדכא סבבים חוזרים של מחאות נגדו ומסייעת לו לבצר את יציבותו לטווח הארוך.

תקיפות CNI (תודעה). השימוש הנרחב של איראן במבצעי תודעה רק הולך וגדל. כמה מן המבצעים ניסו ליצור שסעים ומחלוקות פנימיות ולהחריפם, להשפיע על תהליכי בחירות ולערער את החוסן החברתי במדינת היעד, כפי שהוכיחו התקיפות החוזרות של איראן על מערכות הבחירות בארצות הברית ובישראל. תקיפות אחרות נועדו לשבש את היחסים בין מדינות ולהצית משברים שיש בכוחם להסלים, לעיתים אף לרמה הגרעינית, כמו במקרה של ישראל ופקיסטן. היו גם תקיפות שגרמו לנזק כספי לחברות פרטיות בעולם ולפגיעה במוניטין שלהן. אולם עד כה אף לא אחת מהן התקרבה להיקף ולתחכום של התקיפות שניהלה רוסיה נגד מערכת הבחירות האמריקנית ב־2016, ובפועל יעילותן הייתה מוגבלת. לא ידוע גם על מבצעי תודעה איראניים בסייבר ששיבשו תהליכים פוליטיים וממשלתיים חשובים או שעוררו מחלוקת חברתית גדולה. למרות זאת מספר התקיפות הללו עולה והדאגה גוברת.

מבצעי תודעה בסייבר הם מרכיב במאמצי המשטר האיראני לשמר את שלטונו, והם סיפקו לאיראן ולשלוחיה מגוון פלטפורמות יעילות להגיע דרכן למספר עצום של אנשים ברחבי העולם באופן ישיר ומיידי ובעלות מינימלית. מבצעי הסייבר גם סיפקו לאיראן כלים חדשים ובעלי ערך ליצירת לחץ בינלאומי על ישראל לעצור או לצמצם פעולות צבאיות

בטרם תשיג את יעדיה – הייתה להם השפעה שלילית על יכולתה של ישראל לנהל מלחמה ביעילות ועל מעמדה הבינלאומי.

תקיפות משולבות. השימוש הגובר בתקיפות CNA, CNE ו־CNI משולבות, לרוב גם עם תקיפות כופרה, הניב לאיראן תוצאות טובות למדי. דוגמה מייצגת היא ההפצה באינטרנט של מידע אישי על חברי קהילת הלהט״ב בישראל ועל כל חיילי חטיבה לוחמת של צה״ל. השימוש הרווח בתקיפות כופרה לשם השגת מידע ולא לשם רווח כספי הוא מאפיין ייחודי של העימות בין איראן לישראל.[196]

דרך הפעולה של איראן בסייבר עד כה שופכת אור על שלוש סוגיות קריטיות שהעסיקו את אנשי הביצוע בתחום הסייבר ואת התאורטיקנים. ראשית, היא מוכיחה את החשיבות שמייחסת איראן לתחום הסייבר לא רק משום היותו אמצעי להשגת יעדיה הפוליטיים והצבאיים, אלא גם משום שבשימוש בו יש סיכון נמוך להסלמה. במהלומות ההדדיות בין איראן לישראל בממד הסייבר ובממד הקינטי נראה שסכנת ההסלמה לא הרתיעה במידה רבה מפני המשך התקיפות או מפני עליית מדרגה בהן.

במבט לאחור, לאיראן הייתה סיבה טובה שלא לחשוש מהסלמה. הניסיון מלמד שארצות הברית הגיבה לתקיפות סייבר באמצעים קינטיים בשתי הזדמנויות בלבד, אף לא אחת מהן נגד איראן. על פי דיווחים, ישראל הגיבה לתקיפות סייבר באמצעים קינטיים רק פעמיים, בשני המקרים נגד חמאס, והשתמשה באמצעי סייבר בתגובה לתקיפות סייבר במקרים בודדים בלבד.[197] לפי דיווחים, ישראל אכן הגיבה לתקיפה האיראנית על מערכת המים שלה בתקיפה קשה יותר על נמל איראני; על תקיפה זו הגיבה איראן בתקיפות נוספות, אם כי מוגבלות בבירור, על מערכת המים של ישראל ועל מטרות אחרות. אולם שום צד לא המשיך להסלים. התקיפות המשולבות שאיראן ניהלה נגד ישראל בשנים האחרונות היו ללא ספק משבשות ויקרות, אבל לא קרובות להסלמה כמו מתקפות על תשתיות חיוניות או על מטרות צבאיות.

שנית, אם אכן נכונה הטענה כי רוב היעדים המערביים והישראליים החשובים מוגנים ברמה החורגת מיכולותיה של איראן, היא תומכת באסכולה המקצועית הטוענת כי הסייבר

196 Microsoft Threat Intelligence, ״Iran Turning to Cyber-Enabled Influence Operations For Greater Effect,״ May 2, 2023; Dolev and Siman-Tov, ״Iranian Cyber Influence Operations.״

197 Borghard and Lonergan, ״Cyber Operations״; Catalin Cimpanu, ״Israel Bombed Two Hamas Cyber Targets,״ *The Record,* May 19, 2021; BBC Staff, *BBC*, June 9, 2021; Tal Shahaf, *Ynet*, May 21, 2021.

הופך בהדרגה לכלי הגנתי במקום התקפי. כאמור, יש גם הסבורים שיכולתה של איראן לגרום לנזק משמעותי לשחקניות סייבר מתוחכמות אף פוחתת.

שלישית, לעומת מומחי הסייבר הטוענים שעולם הסייבר מחזק שחקניות חלשות בשל האמצעים האסימטריים הנוספים שהוא מעמיד לרשותן כדי להתמודד עם עוצמתן הגדולה של יריבותיהן, יש מומחים הגורסים כי היכולות הטכנולוגיות המתוחכמות הנדרשות לשימוש יעיל בסייבר רק מחזקות את המדינות המתקדמות ממילא. נראה כי הניסיון במקרה האיראני מטה את הכף לטובת האסכולה השנייה. השימוש של איראן ביכולות הסייבר שלה הוא בהחלט מרכזי, אבל נראה שישראל, ארצות הברית ומדינות המערב מנצלות את הסייבר לצרכים סוציו־אקונומיים, דיפלומטיים וצבאיים רבים יותר. יתרה מזו, מדינות אלו מנצלות היטב כמה מן היתרונות הצבאיים האסימטריים שהסייבר מעניק לאיראן נוסף על הפעלת היכולות הקינטיות החזקות שלהן, ולכן נהנות משני העולמות. במילים אחרות, בשקלול הכולל הכף נוטה לטובת המדינות המתקדמות.

רביעית, אם הערכת איום הסייבר האיראני מתבססת על מספר התקיפות המוצלחות החשובות שהתרחשו עד היום ועל התוצאות שהן גרמו בפועל, אזי האיום הוא משמעותי אך מוגבל. מנגד, אם ההערכה מתבססת על הפוטנציאל הריאלי לשיבוש ולנזק עתידיים, אזי אי אפשר להתעלם מן האיום המתעצם. לכן לישראל אין ברירה אלא להמשיך להשקיע במערכת הסייבר האקולוגית שלה, בהגנת הסייבר האזרחית וביכולות צבאיות הגנתיות והתקפיות.

אסטרטגיית הסייבר של המגזר הציבורי והפרטי בישראל הייתה מן הראשונות מסוגה והתבססה על החלטות הממשלה שהתקבלו בשנים 2011–2015. אלא שהרבה השתנה מאז, ונדרשת בחינה מחודשת ומעמיקה. עם התחומים המחייבים בחינה מחודשת נמנים, בין היתר, המערכת הרגולטורית, המערכת האקולוגית, החוסן המערכתי, שיתוף הפעולה הבינלאומי והתיאום בין הגורמים השונים. האסטרטגיה החדשה חייבת לכלול יעדים ברורים ותוכנית עבודה רב־שנתית המבוססת על אמות מידה מוגדרות היטב.

צה״ל גיבש דוקטרינת סייבר מבצעית, אך לא אסטרטגיית סייבר צבאית כוללת. יתרה מזו, חלפו כבר שמונה שנים מאז החליט צה״ל להקים פיקוד סייבר מאוחד, ואז השהה את ההחלטה עד לבחינה נוספת.[198] כדי למקסם את יכולות הסייבר של ישראל, על צה״ל

198 Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, *Israel and the Cyber Threat: How the Start-Up Nation Became a Global Cyber Power* (Oxford: Oxford University Press, 2023), 250, 256, 257, 309.

לגבש אסטרטגיית סייבר צבאית כוללת ולשלבה עם שאר מרכיבי הכוח הלאומי של ישראל לכדי אסטרטגיית ביטחון לאומי אחת כוללת. יכולות סייבר אינן עומדות בפני עצמן, ואין להתייחס אליהן כך. על התשובה לשאלה כיצד ייראה מבנה הכוח החדש יש מחלוקת; כך או כך, יש לתת מענה לסוגיה.

כיום אין פורום סטטוטורי הכפוף לממשלה ואחראי בפועל לקביעה ולתיאום של סדרי העדיפויות הצבאיים והמודיעיניים בסייבר, לשילוב אסטרטגיות הסייבר האזרחיות והצבאיות ולהקצאת האחריות הארגונית ליישומן. אומנם יש הסדר בלתי פורמלי,[199] אבל הוא אינו ממצה את הפוטנציאל של ישראל, ויש לעדכנו.

את הבסת היריב, במובן המסורתי של שלילת יכולתו או ערעור רצונו להמשיך להילחם, אי אפשר להשיג באמצעי סייבר בלבד. במקום זאת, ישראל צריכה לחתור ל"עליונות סייבר" – היכולת להסב פגיעה או נזק ליריב שיהיו בלתי נסבלים בעבורו, או להפחית את חומרת התקיפות על ישראל לרמה שתאפשר לה להמשיך לתפקד ללא הפרעה ניכרת. אבל גם עליונות סייבר אינה עומדת לבדה, ויש לשאוף לעליונות מצטברת רב־תחומית,[200] כלומר ליישום הדרגתי מצטבר של כל מגוון היכולות העומדות לרשות ישראל (סייבר, קינטיות, דיפלומטיות וכלכליות). עליונות סייבר מודיעינית חשובה במיוחד בסביבת האיומים הקשה והייחודית של ישראל, הן למטרות התרעה מוקדמת והן ליכולות המודיעין הכוללות שלה.

שמירה על עליונות סייבר פירושה טיפוח מאגר לאומי של אנשי הסייבר המוכשרים ביותר בתחום האזרחי, המסחרי, האקדמי והצבאי, אלא שישראל מתמודדת עם מחסור ניכר בהון אנושי זה.[201] יש לפתח את תחום הסייבר בבתי הספר, באוניברסיטאות ובתוכניות ההכשרה למבוגרים. על צה"ל וסוכנויות המודיעין להמשיך לבחון דרכים חדשות לגיוס, להכשרה ולשימור של כוח אדם. הפיתוי של המגזר הפרטי, בארץ ובחו"ל, נותר אתגר לא מבוטל.

ישראל חייבת לגבש אסטרטגיה לאומית להתמודדות עם מבצעי תודעה חתרניים בסייבר שנועדו להחריף מתחים חברתיים, להשפיע על השיח הציבורי ולשבש תהליכי בחירות. ארצות הברית, בריטניה וצרפת הן רק חלק מן המדינות הדמוקרטיות שהחלו לטפל באיום זה, וישראל יכולה ללמוד מן הניסיון שלהן.

תוכנית הגרעין האיראנית נותרה האיום הצבאי הגדול ביותר על הביטחון הלאומי של ישראל. "דוקטרינת בגין" לעצירת תפוצת הגרעין יושמה עד היום פעמיים בלבד, נגד תוכנית

199. Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 259.
200. Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 79–80.
201. Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 198.