המכללה לביטחון לאומי

מחזור מ"ז 2019-2020

**שילוב חברות פינטק בפעילות המערכת הפיננסית והשפעתן על מרחב הסייבר**



מגישים: רו"ח סימה שפיצר\*

 רו"ח הראל שרעבי\*\*

מרצה: פרופ' אביתר מתניה

 **מנהלת יחידת רישוי ובנקים חדשים, הפיקוח על בנקים, בנק ישראל\***

**\*\* סגן בכיר לממונה על שוק ההון, הביטוח והחסכון**

אפריל 2020

1. **מבוא**

בשנים האחרונות עברו מערכות הבנקאות, הביטוח והפיננסיים מהפיכה בסוגי פעולותיהם ושירותיהם. הגופים הפיננסים הרחיבו באופן ניכר את התלות שלהם באמצעים הטכנולוגים עימם הם מנהלים את פעילותם, יוצרים קשר עם לקוחותיהם ומנהלים את סיכוניהם. ההתפתחויות הטכנולוגיות מביאות עמן שירותים דיגיטליים מתקדמים, שיפור חוויית השירות, שירותים ופעילויות מתוחכמים, מיידים וזמינים, אך מנגד הן חושפות את המוסדות הפיננסיים לסיכונים נרחבים ומשמעותיים יותר.

בעבודתנו זו, המונח "**גופים פיננסים**" מתייחס לגופים הבאים: בנקים, חברות כרטיסי אשראי, הגופים המוסדיים (גופי הפנסיה, הביטוח, קופות גמל וקרנות ההשתלמות) וגופים פיננסיים אחרים (מנהלי תיקים, חתמים, יועצים וכו'). **המערכת הפיננסית:** מכלול השווקים בהם פועליםהגופים הפיננסים, והכוללים את שוקי הכספים, מטבע החוץ, המניות, איגרות החוב, נגזרים ומערך התשלומים והסליקה. שווקים אלו מופעלים ומפוקחים על ידי בנק ישראל והבורסה לניירות ערך. המונח "**פינטק**" הוגדר על ידי ה-Financial Stability Board בשנת 2017 כ"חדשנות טכנולוגית בתחום השירותים הפיננסיים, אשר באה לידי ביטוי במודל עסקי חדש, יישום חדש, תהליך או מוצר שיש לו השפעה משמעותית על אספקת שירותים פיננסיים".

כותבי עבודה זו הם רגולטורים מתחומי הפיקוח על הבנקים והפיקוח על שוק ההון, הביטוח והחיסכון. בעבודתנו בחנו סוגיות מתחום הגנת הסייבר הלאומית על הגופים הפיננסים, וערכנו דיון בדבר שילוב חברות פינטק במערכת הפיננסית וההשלכות של שילובן על מרחב הסייבר הפיננסי הלאומי, תוך מתן המלצה לאופן השילוב הראוי.

להלן נושאי העבודה: בסעיף 2 נציג את חשיבות החוסן הפיננסי הלאומי; בסעיף 3 נפרט אודות רגישות המערכת הפיננסית; בסעיף 4 נרחיב אודות רגישות המערכת הפיננסית למרחב הסייבר; בסעיף 5 נסביר אודות חשיבות הרגולציה כאמצעי להגנת סייבר, בסעיף 6 נדון בדילמה שבהגנת סייבר לאומית על עסקים בעלות פרטית; בסעיף 7 נפרט אודות הקמת מרכז סייבר ורציפות פיננסית; בסעיף 8 נדון בדילמות העולות מהתקשרות גופים פיננסים עם חברות פינטק שאינן נתונות לפיקוח ולרגולציה ובסעיף 9 נתייחס למסקנות העולות מעבודתנו ונציע המלצה לפיתרון.

1. **חשיבות החוסן הפיננסי הלאומי**

המערכת הפיננסית ממלאת כיום תפקיד מרכזי במשק, ולכן תפקודה התקין ויציבותה חיוניים להתפתחות המשק ולמיצוי פוטנציאל הצמיחה שלו. המתווכים הפיננסיים אחראים להעברה יעילה של כספי החוסכים ללווים, וכך הם מממנים את ההשקעות ואת הפעילות השוטפת של המגזר העסקי ושל משקי הבית. החברות הפיננסיות מתווכות גם בין החוסכים לממשלה, ובעידן הגלובליזציה גם בין חוסכים למשקיעים בארץ ובחו"ל. התפתחותם ושכלולם של השווקים הפיננסיים הם מן הגורמים החשובים ביותר לתהליך הצמיחה הכלכלית והפריון בארצות המפותחות.

מערכת פיננסית מפותחת וחופשית מאפשרת זרימה יעילה של הון לטובת פיתוחם של עסקים חדשים או הרחבת של עסקים קיימים, ולמעשה מאפשרת את ה"דלק" הנדרש להמרצת הצמיחה במשק. ללא זרימה חופשית של הון יזמים יתקשו למצוא מימון למיזמים חדשים והכלכלה לא תתפתח.

ואולם, תנאי בסיסי לפעילות של מערכת פיננסית הוא האמון שהציבור רוחש לה. ללא אמון, חוסכים לא יהיו מוכנים לתת את כספם לגורם זר מאחר שאין להם אמון שהמערכת הפיננסית תבטיח את החזרת הכסף. ואין זה משנה אם אי החזרת הכסף תהיה תוצאה של מעילה, פשיטת רגל, או כשל תפעולי.

לאור החשיבות שיש למערכת הפיננסית ליציבות המשק ולשגשוגו, לפגיעה בה וכתוצאה מכך פגיעה באמון בה, עלולות להיות השלכות חמורות על פעילותם של משקי הבית והחברות העסקיות במשק. יתרה מזו, התמוטטות של מתווך פיננסי, גם אם הוא קטן (כמו בנק למסחר), עלולה לפגוע ביציבותם של מתווכים אחרים ולגרום לתגובות שרשרת חמורות. קיימת רגישות גבוהה במיוחד לפעילותם של בנקים, משום שהם מהווים את הערוץ המרכזי למערכות התשלומים, לאשראי ולחיסכון. הרגישות הגבוהה של המערכת הפיננסית מחייבת רמת אמינות גבוהה ביותר, משום שגם התערערות קלה ביציבות המתווכים הפיננסיים יכולה למוטט אותם. החשש שיציבותו של מוסד פיננסי נמצאת בסכנה עלולה להביא לידי בריחת מפקידים ולהגדיל את הסיכוי למימוש החשש. כדי לצמצם את הפגיעוּת של המתווכים הפיננסיים למשבר ולמנוע את השלכותיו על המשק כולו, הוקמו בעולם מערכות ציבוריות רגולטוריות להסדרת הפעילות של המתווכים הפיננסיים ולפיקוח על פעילותם. מטרת העל של ההסדרה והפיקוח היא הגנה על האינטרסים של הציבור. ההסדרה מתבטאת בקביעת כללי פעולה בקשת רחבה של תחומים שנועדו להבטיח את השגת מטרה זו.

1. **רגישות המערכת הפיננסית למרחב הסייבר**

בשנים האחרונות התחוללו שינויים בסביבה העסקית, ועמם התפתחו והתעצמו סיכונים, שמקורם בהתפתחות הטכנולוגיה, ברגולציה ובחקיקה מואצת בארץ ובעולם, בתמורות במערכת הפיננסית העולמית ובשינויים בהעדפות הצרכנים ובהתנהגותם. עם סיכונים אלו נמנים סיכון הסייבר והסיכון התפעולי.

הגופים במערכת הפיננסית שבעבר ניהלו מערכות מבודדות, נפתחו לרשת הגלובלית כדי להעניק שירות טוב יותר ללקוחות שמצפים לקבל שירות באמצעים דיגיטליים. הגופים הפיננסים נקטו בצעדי התייעלות והחליפו מערכות טכנולוגיות בעובדים ועל כן הפכו לתלויים במערכות אלו. בנוסף, התחרות הגוברת מצד ענקי הטכנולוגיה כמו אמזון וגוגל ומצד גופים אחרים אינה מאפשרת לגופים הפיננסיים להישאר מאחור במגוון השירותים, זמינותם ונגישותם לציבור. הגופים הפיננסיים אוספים ומחזיקים מידע רב על לקוחותיהם. המידע הזה בעל ערך לגופים הפיננסיים, אך גם לאחרים, וככל שגופים פיננסיים אוספים יותר ויותר מידע על הלקוחות הם יוצרים מרחבי חשיפה חדשים.

רגישות המערכת הפיננסית למרחב הסייבר גבוהה מכמה סיבות. האחת, הגופים הפיננסיים אמונים על החזקת הנכסים הפיננסיים של הציבור והם מחזיקים ומנהלים סכומים עצומים. לכן הם מטרה נחשקת לצורכי עשיית עושר על ידי גורמים פליליים ואחרים. השנייה, מאחר שהפעילות הכלכלית במשק תלויה במערכת הפיננסית, מי שמעוניין לפגוע במדינה עלול לנסות לפגוע במערכת הפיננסית. השלישית, המערכת הפיננסית תלויה באמון הציבור בה, לפגיעה במערכת פיננסית גם את לא נגרם לה נזק כספי ישיר יש אפקט של פגיעה במוניטין ובאמון שגורר בעקבותיו נטישת לקוחות הגורמת לקריסת הגוף הפיננסי, ובעקבותיו נוסר "אפקט דומינו" של קריסת גופים נוספים.

התממשותם של סיכוני סייבר עלולה לשבש את פעילותם התקינה והמאובטחת של גופים פיננסים ולגרום, בין היתר, למניעת שירות, לחשיפת מידע עיסקי או מידע על לקוחות, למחיקה ושיבוש נתונים ועוד. מאפיין מהותי בניהול סיכונים הוא פוטנציאל הפגיעה. פוטנציאל הפגיעה בסייבר מתבטא לא רק בנזק למידע בהקשר של זמינות השירות, שלמות הנתונים וסודיותם, אלא גם בהיבטים הנוגעים לסיכונים אחרים, כגון: מוניטין, סיכונים משפטיים והמשכיות עסקית.[[1]](#footnote-1)

בשנים האחרונות פעלו גורמי הפיקוח בתחום הפיננסי כדי לבחון ולשפר את התמודדות המערכת הפיננסית עם סיכון זה, בין היתר באמצעות רגולציות ייעודית בהיבטי סייבר, עריכת תרגילי סייבר לשם שיפור ההיערכות של התאגידים הפיננסיים מול האיומים השונים ויכולתם להתמודד עמם, הגדרת תרחישי קיצון לשם קביעת התיאבון לסיכון בנושא זה, ביקורות, סקירות והנחיית המערכת לסגירת פערים, מערך דיווחים לפיקוח, שיתוף מידע וכן הגברה ומיסוד שיתוף הפעולה עם מערך הסייבר הלאומי, כדי שאלה יהוו "שכבה נוספת" בהגנה על כספי המפקידים והחוסכים ויציבות המערכת הפיננסית נגד אירועי סייבר.

1. **אירועי סייבר במערכת הפיננסית**

מרחב הסייבר מותקף באופן שוטף ועל בסיס יומי. תוקפי סייבר משקיעים מאמצים רבים באיתור פרצות וחולשות על מנת לנצלם לטובתם או על מנת לגרום נזק לגוף הנתקף. התוקפים עשויים להיות מדינות, ארגוני טרור, עבריינים ואפילו בני נוער משועממים.

מסקר שערכה המפקחת על הבנקים בקרב הבנקים בשנת 2019 עולה כי לדעת הבנקאים, החשיפה למתקפת סייבר מהווה הסיכון המשמעותי ביותר למערכת הבנקאית, ובפער משמעותי מיתר הסיכונים[[2]](#footnote-2).

בשנים האחרונות הלכו והתגברו ניסיונות התקיפה של האקרים, כאשר הם מכוונים חלק ניכר ממאמציהם כנגד גופים פיננסיים. באפריל 2016 פורסם כי האקרים, ככל הנראה מצפון קוריאה, פרצו למערכת הסוויפט, המשמשת כמערכת מאובטחת להעברת כספים בין בנקים, וגנבו מחשבון הבנק של בנגלדש שהוחזק בבנק הפדרל ריזרב בניו יורק 81 מיליון דולר.

גם בישראל, התרחשו מספר אירועים של ניסיונות סחיטה כנגד חברות פיננסיות - ניסיון סחיטה של חברת כרטיסי האשראי לאומי קארד, על ידי עובד לשעבר של החברה; בבנק יהב, ניסיון סחיטה על ידי עובד של ספק חיצוני של הבנק. בנוסף, בבנק ירושלים אירע דלף של נתוני לקוחות בשל אי עמידה בסטנדרטים מאתר המסחר של הבנק.

1. **רגולציה כאמצעי להגנת סייבר במערכת הפיננסית**

רגולציה במרחב הסייבר היא אתגר הנמצא בהתהוות. ענף הפיננסים הוא מרחב מורכב ודינאמי הנשען על המגזר העסקי-פרטי והינו בעל פוטנציאל לגרימת נזק רב לביטחון הלאומי. חוסנו של המגזר הפיננסי במרחב הסייבר קשור ישירות לביטחון הלאומי, אך הוא מהווה חוליה חלשה דרכה מתפתחת מתקפה קיברנטית. סקירה שערכו ד"ר גבי סיבוני ועידו סיוון – סביליה מצביעה על שונות גדולה בסוג ובאופי הרגולציה על נושא הסייבר בין המדינות השונות, ועל היעדר חוק מקיף לנושא הסייבר בישראל.[[3]](#footnote-3) למועד כתיבת עבודתנו, טרם אושרה הצעת חוק הגנת הסייבר שפורסם ביוני 2018. הרגולציה על הגופים הפיננסיים, המהווים גופים פרטיים מבוצעת באמצעות הרגולטורים הייעודיים.[[4]](#footnote-4) עם זאת, המפקח על הבנקים פרסם במרץ 2015 הוראת ניהול בנקאי תקין בנושא "ניהול הגנת הסייבר", אשר קבעה עקרונות יסוד להגנת הסייבר לתאגידים בנקאיים ולחברות כרטיסי אשראי, ובכללן, מינוי מנהל הגנת סייבר, כללי ממשל תאגידי, אסטרטגיה, תהליכי ניהול סיכונים (הכוללים זיהוי והערכת סיכונים), ביסוס מערך בקרות אפקטיבי, ניטור, זיהוי ותגובה לאירועי סייבר, עריכת תרגולים ומערך דיווחים (כולל דיווחים לפיקוח על הבנקים).[[5]](#footnote-5) המפקח על שוק ההון והביטוח פרסם באוגוסט 2016 חוזר מס' 2016-9-14 שנושאו "ניהול סיכוני סייבר בגופים מוסדיים".[[6]](#footnote-6) גם חוזר זה קובע כללים דומים בנושא הגנת הסייבר.

1. **הדילמה שבהגנת סייבר לאומית על עסקים פיננסיים בבעלות פרטית וציבורית**

גופים פיננסיים הם גופים בבעלות פרטית שמנהלים את עסקיהם על מנת להשיא רווח לבעלי המניות שלהם. גופים אלו מנהלים סיכונים רבים ושונים, והם מנהלים אותם בעצמם ועל חשבונם. נכון אמנם שהרגולציה קובעת לגופים כללים לגבי ניהול סיכונים אולם הדבר נעשה בשל העובדה שגופים אלו מנהלים את הנכסים הפיננסיים של הציבור ועל כן נדרש פיקוח ממשלתי. ועדיין גם כאשר הרגולציה קובעת כללים שהגופים צריכים לפעול על פיהם, אין הממשלה מממנת או נוטלת חלק בהגנה מפני הסיכונים השונים.

יש לשאול האם דינו של הסיכון הנובע ממרחב הסייבר שונה בעניין זה מהסיכונים האחרים ויש צורך בהגנת סייבר לאומית או שגם לגביו יש לפעול בדרך דומה ולתת לגופים הפיננסיים להסתדר בכוחות עצמם ועל חשבונם?

הטיעונים **בעד הגנת סייבר** לאומית הם:

1. מרחב הסייבר הוא מרחב שבו יש חיבוריות גבוהה מאוד. פגיעות בגורם מסוים במערכת עלולה להביא לפגיעה גם בגורמים אחרים המחוברים אליו. לדוגמה אם בוצעה חדירה למערכות של חברת ביטוח הדבר עלול להתגלגל לחדירה לתוך מערכות המסלקה שמקשרת בין גופים שונים במערכת הביטוח הפנסיוני. לכן, ומאחר שההגנה היא אינטרס מערכתי ולא רק ספציפית של גוף מסוים, יש חשיבות שהיא תיעשה ברמה הלאומית שתבטיח הגנה מיטבית.
2. כפי שצוין לעיל, הפעילות הכלכלית תלויה במערכת הפיננסית. פגיעת סייבר בגוף פיננסי עלולה להביא לפגיעה בפעילות המשקית. לכן, הגנה לאומית בסייבר היא אינטרס של המדינה על מנת להגן על הפעילות הכלכלית במשק.
3. במדינת ישראל, וגם במדינות אחרות, גורמים שמעוניינים לגרום נזק למדינה מנסים לעשות זאת גם דרך פגיעה בתשתיות פיזיות ואחרות כדי להביא לשיבוש הפעילות הכלכלית של המדינה, מוסדותיה ואזרחיה. פגיעה במערכת הפיננסית עלולה לגרום לפגיעה בחוסנה הפיננסי של המדינה ולכן למדינה יש אינטרס להיות שותפה בהגנה כחלק מההגנה על הביטחון הלאומי.
4. בתחום הסייבר יש יתרון גדול בשיתוף ידע מהיר ובגורם מרכזי שרואה את התמונה המלאה ויכול לשפר את ההגנה לאור התובנות שמתקבלות מהתמונה המלאה. כאשר גוף מסוים חווה תקיפת סייבר ויש לו יכולת להתריע על כך במהירות לגורמים אחרים שעלולים להיפגע מכך, יש בכך יתרון גדול. לכן, הגנת סייבר לאומית מגדילה את אפקטיביות ההגנה של כל אחד מהגופים, באופן שלא היה מתקבל מפעילות עצמאית של כל אחד מהגופים.
5. מעורבות של המדינה מאפשרת להתגבר על מגבלות של שיתוף פעולה בין גופים מתחרים שבנסיבות אחרות הוא אסור כדי למנוע פגיעה בתחרות בשוק.
6. תקיפות במרחב הסייבר הן סוג של פשיעה, ובדומה לסיכונים דומים במרחב הפיזי בהם יש מעורבות מדינתית (משטרה ואחרים) כך גם במרחב הסייבר נכון שהמדינה תהיה מעורבת בהגנה לאומית ותבטיח שמירת חוק וסדר.

הטיעונים **נגד הגנת סייבר לאומית** הם:

1. כאמור לעיל, הגופים במערכת הפיננסית הם גופים פרטיים שפועלים להשאת רווחיהם. הם אינם גופים שבבעלות הממשלה או גופים ללא מטרת רווח. אם הגנה במרחב הסייבר היא צורך הנדרש מהפעילות העסקית שלהם עליהם לפעול בעצמם לשם כך כפי שהם פועלים להגן מפני סיכונים אחרים שנובעים מפעילותם העסקית.
2. יש סיכונים נוספים שעלולים לגרום לגוף פיננסי נזק שיביא לפגיעה בפעילות הכלכלית במשק, ועדיין אין הגנה לאומית מפניו אלא יש כללי רגולציה שדורשים מהגוף ניהול סיכונים. כך למשל, סיכון מעילות והונאות בגוף פיננסי עלול לגרום לקריסת מוסד פיננסי (מקרה בנק למסחר) ועדיין אין הגנה לאומית מפני סיכוני מעילות והונאות.
3. **איגום אמצעים להגנת סייבר במרחב הפיננסי הלאומי והקמת הCERT [[7]](#footnote-7) הפיננסי**

הדיונים בעד ונגד הגנת סייבר לאומית לגופים הפיננסים הוכרעו באמצעות החלטת ממשלה מס' 1815 להקמת מרכז חירום לאומי, הכולל בתוכו מספר מוקדי התמחות, ובכללם CERT פיננסי. בהתאם לאסטרטגיית הסייבר הלאומית, בליבת מאמצי החוסן הלאומיים נמצאים תהליכי שיתוף מידע בין המדינה לארגונים במשק, ובין הארגונים לבין עצמם, באופן המאפשר בלימת תקיפה על ידי העברת תובנות וידע רלבנטיים בין ארגונים שהותקפו והצליחו להתמודד עם התקיפה לבין ארגונים שטרם הותקפו או שטרם הצליחו להתמודד עם התקיפה. שיתוף מידע נדרש ברמה הלאומית אך גם ברמה המגזרית, על מנת לאפשר התמודדות מיטבית עם התקפות סייבר. שיתוף פעולה בתוך המגזר הפיננסי מאפשר בניית אמון והכרות מעמיקה עם הארגונים ועם צורכיהם. גישה זו מאפשרת העמקה בתהליכים, בטכנולוגיות ובסיכונים המאפיינים את המגזר הפיננסי, תוך בחינת הזיקות בין סיכוני סייבר לסיכונים אחרים.[[8]](#footnote-8) לאור זאת, הוקם ביום 4 בינואר 2017, **המרכז לסייבר ורציפות פיננסית** כחלק מהמרכז ה-CERT הלאומי. המרכז מתמקד בתהליכים שהוגדרו על ידי המפקחים. החברות במרכז מיועדת לבנקים, חברות ביטוח, גופי השקעות והבורסה לניירות ערך. החברות במרכז הינה לשיקול דעתו של הגוף הפיננסי, ונובעת מההבנה ששיתוף מידע בתחום הסייבר מהווה מכפיל כוח משמעותי לכלל הגופים. יש לציין כי הגנת הסייבר הלאומית חלה רק על גופים פיננסים בעלי היקף פעילות משמעותי ורק על גופים המצויים תחת פיקוחם של הרגולטורים הפיננסים השונים.

1. **הדילמה הכרוכה בהתקשרות של המגזר הפיננסי מול חברות פינטק חדשניות**

המגזר הפיננסי והרגולטורים שלו ידועים בשמרנותם.

מאידך, ישראל ידועה בחדשנותה הטכנולוגית. על אף שישראל הינה בין המדינות המובילות בעולם במספר חברות הפינטק שהוקמו בה, מרביתן של החברות אינן פעילות בישראל. במשך שנים רבות נמנע המגזר הפיננסי (בעיקר הבנקים, אם כי לא רק), לאפשר לחברות פינטק להתפתח בישראל. חסמים רגולטורים וקשיים מצד המערכת הבנקאית הובילו להקמת צוות עבודה בין משרדי על ידי שר האוצר משה כחלון בשנת 2018.

על פי דוח הצוות הבין משרדי להקמת סביבת ניסוי לחברות טכנולוגיה פיננסית[[9]](#footnote-9), בין יתר הסיבות שמונה הדוח לקשיים של חברות הפינטק, נמנה החשש מסיכוני סייבר בשל חשיפות לסיכונים בשרשרת האספקה של המערכת הפיננסית.

**נשאלת השאלה,** האם על ישראל לעודד כניסת חברות פינטק למערכת הפיננסית **גם במחיר של מתן הקלות רגולטוריות ונטילת סיכונים בשרשרת האספקה של הגופים הפיננסיים?**

השיקולים **בעד מתן הקלות** לצורך הכנסת גופי פינטק למערכת הפיננסית:

1. חדשנות – חברות הפינטק מציעות מוצרים וטכנולוגיות חדשים, לעיתים גם פורצי דרך בחדשנותם. מרבית הפעילות של חברות הפינטק אינן מופנות לשוק הישראלי ובכך קיים הפסד לשוק וללקוחות.
2. הגברת תחרות– כניסת גופים חדשים למערכת הפיננסית תהווה זרז לירידת מחירים ולהגברת התחרותיות של כלל הגופים הפועלים במערכת הפיננסית.
3. התייעלות ושיפור רווחת הלקוחות - כניסת טכנולוגיות חדשות עשויות לצמצם באופן משמעותי את העלויות ללקוחות.

השיקולים **נגד מתן הקלות** ותמיכה בהכנסת פעילות חברות הפינטק:

1. סיכונים הנובעים משרשרת האספקה – גופי פינטק המספקים שירותים למוסדות פיננסים או שמשתמשים במערכת התשלומים או בשירותי הבורסה לניירות ערך עלולים לגרום לגופים עימם הם פועלים לחשיפה לסיכוני סייבר. מסמך של מערך הסייבר הלאומי בנושא "סיכונים במיקור חוץ ושרשרת אספקה"[[10]](#footnote-10) מפרט את הסיכונים הייחודיים לשרשרת האספקה שרלבנטיים גם במקרה זה: א. הכנסה של תוכנה או חומרה הנגועה בנוזקה. ב. ביצוע פעולה זדונית על ידי גורם תחזוקה. ג. ביצוע פעולה זדונית באמצעות ערוץ התחזוקה מרחוק. התוקפים מנצלים את הקלות היחסית לחדור לחברות ולארגונים קטנים יחסית, שיש להם מערך הגנת סייבר מוחלש, כדי לחדור דרכם לארגוני יעד בעלי חשיבות קריטית. תוקפים גם מנצלים את העובדה שלחלק מספקי המשנה של ארגונים קריטיים יש גישה ישירה או קלה יותר אליהם, כדי לחדור באמצעותם לאותם ארגונים.
2. היעדר רגולציה – חברות הפינטק הן בדרך כלל חברות קטנות ודלות משאבים שהתפתחו ללא עמידה בתנאי רגולציה מחמירים, וכך הן עלולות לחשוף את לקוחותיהם ואת המוסדות הפיננסים הפועלים עימם לסיכוני סייבר משמעותיים. בעוד הגופים הפיננסים משקיעים תשומות עצומות להגנה מפני אירועי סייבר, עלולה מערכת האבטחה הנמוכה יחסית של חברות פינטק קטנות, שאינה מחויבת לעמידה ברגולציה מחמירה לשמש יעד לתקיפה של תוקפי סייבר. פעילות חברות אלו ללא רגולציה מחייבת או תחת הקלות משמעותיות יחשפו את הגופים הפיננסיים לסיכונים משמעותיים.
3. היעדר תשומות לעמידה בסטנדרטים גבוהים של הגנת סייבר – עלויות הגנת הסייבר נאמדות במיליוני שקלים עקב הצורך בעמידה בתהליכים בדיקה ועבודה נרחבים. הקלות בתהליכי הגנת סייבר בחברות פינטק המשרתות לקוחות או המהוות חלק ממערכת האספקה עלולות להיות פתח לניצול לרעה לתקיפות סייבר כנגד גופים פיננסיים או כנגד המערכת הפיננסית.

בין ההמלצות שנכללו בדוח הצוות הבין משרדי הוצע להקים סביבת ניסוי רגולטורית, בפיקוח של הרגולטור המתאים ותוך הנחייה וסיוע במסגרת "sandbox", שתכלול רגולציה מקלה המותאמת לגודל החברה ולסיכוניה וכן מעבדת חדשנות בתחום ה"פינטק-סייבר", שתוקם בתוך רשות החדשנות, בשילוב עם מערך הסייבר הלאומי ומשרד האוצר.

על מנת לאפשר הקלות אלו נדרשים תיקוני חקיקה והתאמות רגולטוריות. בשל העדרה של פעילות ועדות הכנסת, לא הושלם הדיון בדוח זה ולא אושרו תיקוני החקיקה שהוצעו בו.

1. **סיכום ומסקנות**

בעבודתנו הצבענו על החשיבות הרבה של החוסן הפיננסי לביטחון הלאומי ועל כך שפעילות תקינה של שווקי הכספים וההון ושל המוסדות הפיננסים הכרחית לצורך שמירה על יציבות פיננסית והמשכיות עסקית כלכלית. המערכת הפיננסית הינה אחת מהיעדים המותקפים ביותר על ידי גורמי סייבר ולכן היא מצויה תחת הנחיות וסיוע של ה-CERT הפיננסי, בכפוף להנחיות הרגולטורים. קיימת חשיבות רבה לרגולציה בתחום הגנת הסייבר המוטלת על הגופים הפיננסים, אשר מאפשרת עמידה בתקנים מחמירים שנועדו להגביר את עמידות המערכת הפיננסית לסיכוני סייבר ולצמצם את פגיעותה.

בשנים האחרונות הרגולטורים המובילים בישראל הבינו את החשיבות שיש לכניסת גופים חדשים למערכת הפיננסית, אשר תורמים לחדשנות, לשיפור חווית השירות ללקוחות ולהתייעלות המערכת הפיננסית, על מנת להתאים עצמה לתחרות הגוברת מצד ענקיות הטכנולוגיה. בד בבד, הלכה והתפתחה בשנים האחרונות תעשיית פינטק ישראלית, המתקשה לפעול במערכת הפיננסית הישראלית בשל קשיים שהיא מערימה על גופים אלו. ניתן לציין כי המפקחים אף עודדו הקמת בנקים וחברות ביטוח חדשניים, ופעלו למתן הקלות בתחומים שונים, תוך שמירה על מסגרת רגולטיבית מוסדרת.

מתן הקלות גורפות לחברות הפינטק, בפרט בנושא הגנת הסייבר עלול לסכן את המערכת הפיננסית. ללא עמידה בסטנדרטים של הגנת סייבר, פעילות חברות אלו עלולה להוות חשיפה לפגיעה משמעותית בחברות עצמן, בלקוחותיהן ואף בכלל המערכת הפיננסית. עם זאת יש חשיבות רבה בחדשנות הטכנולוגית ומדינת ישראל אינה יכולה להישאר מאחור. לכן, יש לייצר פתרונות מותאמים לפעילותם של גופי פינטק באופן שלא יחשוף את המערכת כולה לסיכוני סייבר. הקמת sandbox, בכפיפות לרגולטורים הרלבנטיים, תוך קביעת מסגרת רגולטורית מותאמת ובהכוונה של מערך הסייבר הלאומי עשויה להוות דוגמה לפתרון שכזה.

100

עבודה מצוינת. הצגת הנושא, חשיבותו והדילמות השונות הנוגעות לשילוב והקלה על חברות הפינטק ברורה, מקיפה ומסומכת היטב.

**ביבליוגרפיה**

**מחקרים:**

1. סיבוני וקליין (2018). קווים מנחים לניהול סיכוני סייבר, עמודים 24-25. סייבר מודיעין וביטחון, כרך 2 גיליון 2. INSS, המכון למחקרי ביטחון לאומי, אוניברסיטת תל-אביב.
2. סיבוני וסיון-סביליה (אוגוסט 2018). *רגולציה במרחב הסייבר*, עמודים 81-84.
3. "סיכונים במיקור חוץ ושרשרת אספקה", מערך הסייבר הלאומי, 18 במאי 2017.

**מסמכי מערך הסייבר הלאומי:**

1. האסטרטגיה הישראלית להגנת הסייבר, משרד ראש הממשלה, מערך הסייבר הלאומי, עמוד 17.

**הוראות רגולטוריות וסקירות פיקוחיות:**

1. סקירת הפיקוח על הבנקים לשנת 2018, עמודים 14-15.
2. הוראת ניהול בנקאי תקין מס' 361 בנושא "ניהול הגנת הסייבר" מיום 16 במרץ 2015.
3. ניהול סיכוני סייבר בגופים מוסדיים, חוזר מוסדיים מיום 31 באוגוסט 2016 מס' 2016-9-14.
4. דוח הצוות הבין משרדי לבחינת הקמתה של סביבת ניסוי לחברות טכנולוגיה פיננסיות, ינואר 2019.
1. סיבוני וקליין (2018). *קווים מנחים לניהול סיכוני סייבר*, עמודים 24-25. סייבר מודיעין וביטחון, כרך 2 גיליון 2. INSS, המכון למחקרי ביטחון לאומי, אוניברסיטת תל-אביב. [↑](#footnote-ref-1)
2. סקירת הפיקוח על הבנקים לשנת 2018, עמודים 14-15. [↑](#footnote-ref-2)
3. סיבוני וסיון-סביליה (אוגוסט 2018). *רגולציה במרחב הסייבר*, עמוד 81. [↑](#footnote-ref-3)
4. שם, עמודים 81-84. [↑](#footnote-ref-4)
5. הוראת ניהול בנקאי תקין מס' 361 בנושא "*ניהול הגנת הסייבר*" מיום 16 במרץ 2015. [↑](#footnote-ref-5)
6. *ניהול סיכוני סייבר בגופים מוסדיים*, חוזר מוסדיים מיום 31 באוגוסט 2016 מס' 2016-9-14. [↑](#footnote-ref-6)
7. - Computer Emergency Response Team - CERT צוות חירום לטיפול באירועי מחשב. [↑](#footnote-ref-7)
8. האסטרטגיה הישראלית להגנת הסייבר, משרד ראש הממשלה, מערך הסייבר הלאומי, עמוד 17. [↑](#footnote-ref-8)
9. *דוח הצוות הבין משרדי לבחינת הקמתה של סביבת ניסוי לחברות טכנולוגיה פיננסיות*, ינואר 2019. גילוי נאות – סימה שפיצר, המעורבת בכתיבת עבודה זו, השתתפה בדיוני הוועדה ובכתיבת הדוח. [↑](#footnote-ref-9)
10. "סיכונים במיקור חוץ ושרשרת אספקה", מערך הסייבר הלאומי, 18 במאי 2017. [↑](#footnote-ref-10)