

פרו-אקטיבי? האם ניתן לתקוף כדי להגן על מערכת

מאת: עו"ד יהונתן קלינגר

הקדמה

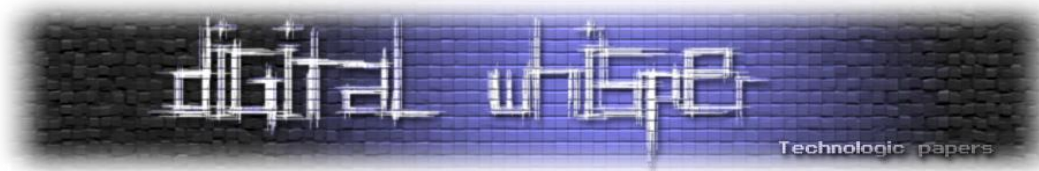
בסופו של דבר, מלחמות ההאקרים הישראלים בעוכרי ישראל רק יפגעו בנו, ולא מדובר על יותר מאשר נערי גבעות עם מקלדת.

בשבועות האחרונים, בעיקר בעקבות [פעולתו של ההאקר OxOmar ששחרר לאוויר העולם עשרות אלפי פרטים של אזרחים ישראלים](#), ובכלל זה [פרטי כרטיסי אשראי](#), והכל [ממניעים אידיאולוגיים אנטי-ציוניים](#), החלו פעולות תג-מחיר משני הצדדים שפגעו רק באזרחים. אחרי מספר פרסומים של פרטי אשראי ומידע אישי נוסף של אזרחים ישראלים שגרמו לנזק בלתי הפיך, ויחד עם מרשם האוכלוסין שדלף לאינטרנט ככל הנראה גרועים לא פחות מדליפתו של המאגר הביומטרי בעצמו, החל הצד הישראלי לנקום.

בתחילה [התאגדה קבוצת האקרים פרו-ישראלית](#), שעל פי פרסומיה ניסתה לעבוד בצורה אתית ורק להראות על פגיעות במערכות אבטחת מידע של הצד השני; אלא, שמשוהו קרה. אחד ההאקרים, ככל הנראה בלי ידיעת חבריו לקבוצה, [החל לפרסם מידע אישי של אזרחים סעודים](#), ירדנים ופלשתינאים, והכל מתוך [אידיאולוגית תג מחיר. לדבריו, "אני יודע שהם חפים מפשע \(מעט מתוכם\). אבל ערבים הם ערבים"](#). כלומר, פגיעה באזרחים חפים מפשע היא אמצעי להחזיר לצד השני.

אותה קבוצה, כחבורה של פורעים שלוקחים את החוק לידיים ביצעה לא מעט בשבועות האחרונים, החל מפרסום [כתובות מייל של סעודים](#) ועד [פרסום של "עומר כהן" של פרטי כרטיסי אשראי וכתובות דואר](#). זו לא הפעם הראשונה שישראלים מתנהגים כמו הערס המצוי: היו כבר [פריצות שנועדו לקדם את שחרור גלעד שליט](#) ואפילו [נקמה ב-2005 על השחתת אתרים ישראלים שעלתה בהשחתה של אתרים טורקים](#), אבל זו פעם ראשונה שהנפגעים הם אזרחים חפים מפשע, ולא אתרי ממשלה, אתרים תומכי טרור או ארגוני האקרים אחרים.

אלא, שלא רק שפעילותו של אותו האקר, הגם שנעשית ממניעים אידיאולוגיים, אינה בדיוק חוקית ולא עומדת בקנה אחד עם [חוק המחשבים](#), אלא שפעילותו לא שונות מבחינה חוקית מההאקרים האנטי-ישראלים, וזאת מסיבה אחת: החוק היבש לא נרטב אף פעם.



האם יכול אותו נער גבעות עם מקלדת לקום ולהתגאות במעשיו כאשר סגן שר החוץ של ישראל, **דני איילון**, [קורא למעשים אלה פעילות טרור](#)? האם אין שוני בין פעילותו של ההאקר והדלפת המידע האישי של סעודים, שיכולים אפילו להיות פרו-ישראלים ואנטי-מוסלמים, שכל פשעם היה לרכוש באתר קניות סעודי, לבין פעולה זהה נגד ישראלים? לא.

[פורסם במקור בגרסא ערוכה ב**חורימבהרשת**]

לתקוף על מנת להגן

הבעיה בישראל, ככל שבאמת אפשר להגדיר אותה כבעיה, היא העדר הגנה על פעילות פרו-אקטיבית. לצורך הבנה מהי פעילות פרו-אקטיבית, אני רוצה לחזור להגדרת "כח סביר" שכולנו מכירים בחוק הישראלי. בואו נקח את הדוגמא הפשוטה ביותר, לי יש חצר, ומישהו מנסה להכנס בכח לחצר שלי: במקרה כזה, מותר לי להשתמש בכח סביר ([סעיף 18 לחוק המקרקעין](#)), "תפס אדם את המקרקעין שלא כדין רשאי המחזיק בהם כדין, תוך שלושים ימים מיום התפיסה, להשתמש בכוח במידה סבירה כדי להוציאו מהם" ותקום לי גם הגנה בחוק העונשין אם אני אשתמש באלימות ([סעיף 34ב לחוק העונשין](#)), עפ 8181/09 [מדינת ישראל נ' שחר מזרחי](#)).

בפרשת שחר מזרחי פסק בית המשפט העליון כי שוטר אשר ירה לכיוון של פורץ לרכב, לאחר שהפורץ ברח, אינו מקים את הגנת ההגנה העצמית. בפסק הדין פסק בית המשפט העליון כי:

"פסיקת בית משפט זה העמידה את קיומה של טענת "הגנה עצמית" על פי הוראות חוק העונשין על שישה תנאים שצריכים להתקיים על מנת שתעמוד לנאשם הגנת ההגנה העצמית ... התנאי הראשון הוא **תקיפה שלא כדין**. התנאי השני הוא **קיומה של סכנה מוחשית "של פגיעה בחייו, בחירותו, בגופו, או ברכושו, שלו או של זולתו"**. תנאי נוסף לתחולת ההגנה הוא **מיידיות הסכנה**. משמעותו של תנאי זה היא כי על ההגנה להתבצע רק מרגע שהמעשה דרוש באופן מיידי כדי לעצור את התקיפה, וכי עליה להיפסק מרגע שההתגוננות אינה נדרשת עוד לשם עצירת התקיפה ... התנאי הרביעי לתחולת ההגנה הוא כי **הטוען להגנה לא נכנס למצב בהתנהגות פסולה**" תוך שהוא צופה מראש את אפשרות התפתחות הדברים". תנאי נוסף וחמישי לתחולת ההגנה הוא **תנאי הנחיצות** ... התנאי השישי והאחרון לתחולת ההגנה הוא **תנאי הפרופורציה**. בהתאם לתנאי זה, שמעוגן אף הוא בדרישת הסבירות הקבועה בסעיף 34טז לחוק העונשין, נדרש יחס ראוי בין הנזק הצפוי מפעולת המגן לבין הנזק הצפוי מן התקיפה. היינו, ייתכן מצב שבו אף אם פעולה מסוימת היא הפעולה האפשרית היחידה להדיפת התקיפה היא לא תהיה מוצדקת, כיוון שלא מתקיים יחס ראוי בין הנזק הצפוי מפעולת המגן לבין הנזק הצפוי מן התקיפה."

פרו-אקטיבי? האם ניתן לתקוף כדי להגן על מערכת

www.DigitalWhisper.co.il

כלומר, המחוקק הכיר בזכות הקניין של אדם כשהדבר נוגע לחייו, כשהקנה לו את ההגנה העצמית בדיני העונשין, הכיר בהגנה על קניינו כאשר הגן על המקרקעין שלו ועל רכוש. ולכן נשאלת השאלה, האם המחוקק הגן על קניין וירטואלי של אדם? כלומר, תיאורטית לגמרי, דוקטרינת ההגנה העצמית מאפשרת להכיר בהגנה פרו-אקטיבית כנגד האקרים ולפעול כנגד תקיפה שלא כדין, וזאת כל עוד ההגנה עומדת בכל הכללים המפורטים, לרבות תנאי הפרופורציה.

לא מדובר על המצב האירוני בו לאדם תהא הזכות להכות את חברו רק בגלל שזה לקח שלא ברשות קובץ MP3 שהאדם האחר יצר, או למצב בו ניתנת לאדם הזכות להשמיד אייפון רק בגלל שהוא מחזיק אלבום של תמונות מפרות זכויות יוצרים או פוגעות בפרטיות (למרות, שבתיאוריה לגמרי, אולי ניתן לעשות כן לאחר צו בית משפט בעקבות סעיפים [60 לחוק זכויות יוצרים](#), [29 לחוק הגנת הפרטיות](#) ו-[9 לחוק איסור לשון הרע](#)), אלא על מצב בו איש אבטחת המידע יכול לגרום לנזק לאדם המנסה לחדור למחשב שלו, או להשתמש באותם כלים שהחודר משתמש על מנת להתחקות אחר זהות ההאקר.

הדיון מתחיל בהבדל התיאורטי ביותר בין מאבטח אישי לבין איש אבטחת מידע, שמזכיר קצת את [הדיון בין חוקר פרטי להאקר שהעלתי כבר בגליון קודם של המגזין](#). המאבטח האישי הוא אדם שנשכר לצורך הגנה על חייו של אדם מפני איומים והוא מיומן בהגנה. הוא יכול להפעיל כח סביר כדי למנוע סכנה מוחשית ומיידית. אבל האם יש "מאבטח אישי וירטואלי" שיכול לאתר, בזמן אמת, פגיעה בנכסים הוירטואלים של אדם ולפעול כנגדו? ואם כן, מהם הקריטריונים שמאפשרים זאת?

בפסיקה הישראלית קשה מאוד למצוא אזכורים להגנה עצמית וירטואלית. לא רק שהדבר לא נדון בפסיקה הפלילית, אלא גם שדומה שעד עכשיו לא היו מקרים כאלה. לכן, המקרה התיאורטי שלנו לניתוח יצטרך להיות כזה: אליס בעלים של אתר אינטרנט שמחזיק מידע פרטי על גולשים.

בוב הוא האקר מיומן שמנסה לפרוץ אליה למחשב וצ'רלי הוא איש אבטחת המידע של אליס. לצורך המקרה, צ'רלי איתר בזמן אמת את פעילותו של בוב וחדר, בהסתמך על פרצות אבטחה, למחשבו של בוב ומחק ממנו את הפרטים האישיים של לקוחותיה של אליס רק לאחר שהעתיק במלואו את המידע. לאחר הפעילות, צ'רלי דיווח למשטרה על הפריצה וטען להגנה עצמית.

המשטרה רוצה להאשים את צ'רלי בעבירות של פגיעה בפרטיות, חדירה לחומר מחשב ומחיקת חומר מחשב. האם היא תנצח? כמובן שעד שעניין כזה או דומה לא יגיע לפתחו של בית המשפט אנו לא יכולים להיות ודאיים בנושא, אבל אנחנו כן צריכים לשאול את עצמנו על מה בית המשפט יסתמך.

במקרה כזה לא מדובר על פעילות תג מחיר, אלא על מצב בו אדם לוקח את החוק לידי; השאלה העולה היא מיידיות הפעולה והאם הנזק שיגרם מאי נקיטתה מצדיק את הפעולה מהווה גורם חוקי לכשעצמו. לצורך כך יש לבחון את ששת הקריטריונים להגנה העצמית:

תקיפה שלא כדין. ובכן, אין מחלוקת שכניסה למחשב ונטילת המידע היא תקיפה שלא כדין. [סעיף 4 לחוק המחשבים](#) אוסר על חדירה שלא כדין לחומר מחשב; זהו איסור שכולנו מכירים ויודעים עליו ולמרות מעט מאוד דיון משפטי בנושא, ברור גם לאור הפרשנות המרחיבה ביותר של הסעיף שכניסה ללא רשות לאתר ונטילה של מידע ממנו שלא בהסכמה, כאשר מטרת הנטילה אינה לבדוק את ענייני האבטחה היא פריצה (לדוגמא, פ 9497/09 [פרקליטות מחוז ירושלים נ' משה הלוי](#)).

סכנה מוחשית לפגיעה ברכוש. אכן, חדירה לחומר מחשב ופרסום של המידע או נטילה שלו היא פגיעה בפרטיות ויכולה לגרום לסכנה בפגיעה ברכוש (איכות מסד הנתונים, קניין רוחני וכדומה), או בזכויות חוקתיות אחרות כמו הזכות לפרטיות.

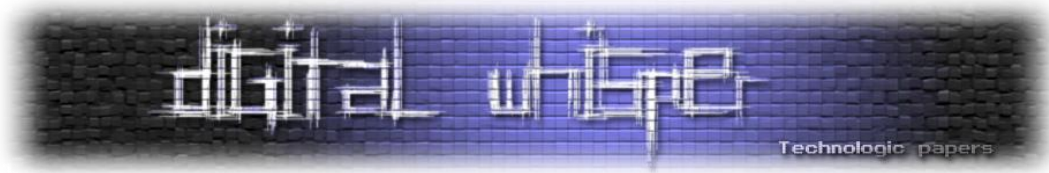
מיידיות הסכנה. שאלת מיידיות הסכנה היא משמעותית כאן; בעצם השאלה היא האם לא היה ניתן לחכות, להתקשר למשטרה ולטפל בסיכון הזה בצורה אחרת, ולא דווקא ללכת ולעבור על החוק. בית המשפט העליון פסק כי "תנאי זה קובע כי על ההגנה להתבצע רק מרגע שהמעשה דרוש באופן מידי כדי לעצור את התקיפה, וכי עליה להיפסק מרגע שההתגוננות אינה נדרשת עוד לשם עצירת התקיפה" (עפ 9878/09 [מדינת ישראל נ' רמי מוסא](#)); כך גם בפרשה אחרת, בה פסק בית המשפט כי "עליו להתבצע רק משעה שהמעשה דרוש באופן מידי על מנת להדוף את התקיפה ולא לאחר הרגע שבו התקיפה אינה מהווה עוד איום" (עפ 6392/07 [מדינת ישראל נ' שמואל יחזקאל](#)). כלומר, יש כאן שאלה של ממש: האם בעצם הפעולה לאחר שהסתיימה התקיפה יכולה לקום הגנת ההגנה העצמית, להבדיל ממצב בו הנפגע מוצא את הפוגע במהלך הפעילות? זו שאלה שאינה טריוויאלית, ויש לקחת את הפרשנות כאן בזהירות.

לא נכנס למצב בהתנהגות פסולה. כאן, לדוגמא, הכניסה לסכנה במצב פסול, כמו [Honeypot](#) כנראה לא תקים את ההגנה הדרושה לצורך ההגנה העצמית. המצב היחיד בו ההגנה תקום היא כאשר מדובר בפריצה שנגרמה לאתר שאינו פרצה שקוראת לגנב לצורך הפעלת אלימות כנגדו.

נחיצות. כלל הנחיצות קובע כי "יש לבדוק האם עמדו למתגונן אלטרנטיבות להדיפת התוקף מלבד שימוש בכוח, ומן הבחינה הכמותית יש לברר האם ניתן היה להפעיל כוח מועט יותר לצורך בלימת התקיפה" (עפ 8208/07 [אבי אלימלך נ' מדינת ישראל](#)); לא להתבלבל עם תנאי הפרופורציה, אבל כלל הנחיצות בודק האם באמת היו אלטרנטיבות אחרות: במקרה של אליס ובוב, עולה השאלה מהן האלטרנטיבות האחרות מלבד פריצה למחשביו של בוב כדי למנוע את הפריצה? בכל מקרה, איני רואה בהכרח אפשרויות אחרות

פרו-אקטיבי? האם ניתן לתקוף כדי להגן על מערכת

www.DigitalWhisper.co.il



מלבד החדירה, כל עוד היא מבוצעת בסמיכות לפריצה: כאשר מדובר על פורצים מיומנים דיו שיכולים להסוות את מיקומם או את חיבורם, וכן להעלם בטווח של כמה דקות, הרי שאלא אם מכת התשובה תבוצע בתוך דקות מספר על ידי פריצה, הרי שלכשתגיע המשטרה לבדיקה לא בהכרח יהיה לה מה לעשות. לכן, ככל הנראה תנאי כזה עשוי להתקיים.

פרופורציה. שאלת הפרופורציה היא משמעותית; הפרופורציה דורשת שהפגיעה תהיה במידה שאינה עולה על הנדרש. השאלות שיעלו כאן הן האם מעבר לפריצה ומחיקה של החומר המקורי יבוצעו פעולות נוספות כמו "תג מחיר" לאותו פורץ, או האם יבוצע ניקוי ומחיקה רק של המידע של אליס; האם הפריצה תבוצע תוך פגיעה גם באחרים חפים מפשע (בניח, מחשבי זומבי בשימוש אותו פורץ) או רק במחשבים של הפורץ.

סיכום

שאלת ההגנה העצמית עדיין עומדת במעורפל כאשר מדברים על הגנה עצמית וירטואלית; יש כאן לא מעט שאלות שבתקווה בית המשפט לא ידון בהם ובתקווה נצליח להמנע מהן. אבל, צריך לזכור שהדרך הנכונה להמנע מדיון כזה היא לפעול למען הגנה עכשיו על מערכות המידע שלנו, ולא לנסות להביא צידוקים בשלב מאוחר יותר לגבי הסיבות בגינן יש לפרוץ למחשביהם של אחרים.