המכון הישראלי
לדמוקרטיה

www.idi.org.il

**26 יולי 2021**

# מצע לדיון בוועדת חוץ וביטחון בעקבות פרשת "פגסוס"

**ד"ר תהילה שוורץ אלטשולר, עו"ד עמיר כהנא, ד"ר רחל ארידור הרשקוביץ**

## 1. הקדמה:

הגילויים באמצעי התקשורת בארץ ובעולם לגבי שימושים לרעה, לכאורה, בטכנולוגיית איסוף המידע באמצעות מערכת "פגסוס" של חברת NSO, ממשיכים להכות גלים. פרשת פגסוס איננה הפתעה ו- NSO איננה החברה היחידה המבקשת לעצמה נתח מן העוגה היוקרתית של טכנולוגיות מעקב ואיסוף. מומחי משפט בינלאומי טוענים כי אנו על סיפה של קטסטרופה גלובלית של מעקב טכנולוגי, ולמרבה הצער מדינת ישראל הופכת להיות פניו של המשבר. זאת, בשני מרחבים – ראשית, מול ידידותיה של ישראל בעולם המערבי ובכללן האיחוד האירופי והאו"ם, ושנית, מול תעשיית הטכנולוגיה המקומית והגלובלית.

במרחב הראשון מתברר כי מדינת ישראל מפקחת באופן הדוק על יצוא טכנולוגיות ביטחוניות אבל מתייחסת בעיקר לשיקולים צרים של יחסים עם מדינות ספציפיות, ומתעלמת מכך שמי שמקבלים לידיהם את המערכת עושים בה שימוש לפגיעה בזכויות אדם. נדרש כרגע שידוד מערכות:

- התחשבות בשיקולי הגנה על זכויות אדם בתהליכי קבלת החלטות;
- הגברת השקיפות של תהליך הרישוי;
- פישוט הרגולציה (רגולציה מסובכת היא מקור להשחתה);

**מר אמיר אלשטיין**
יו"ר הוועד המנהל
**מר יוחנן פלסנר**
נשיא
**מר ברנרד מרכוס**
יו"ר בינלאומי
**פרופ' גרהרד קספר**
יו"ר המועצה הבינלאומית

**חברי הוועד המנהל**
פרופ' ורד וניצקי-סרוסי
מר חן ליכטנשטיין
גב' מזל מועלם
מר סלי מרידור
עו"ד אבי פישר
מר אביעד פרידמן
ד"ר מיכל צור
מר יוסי קוצ'יק
מר עימאד תלחמי

**המועצה הבינלאומית**
השופטת רוזלי סילברמן אבלה, קנדה
מר אליוט אברמס, ארה"ב
ד"ר מרטין אינדיק, ארה"ב
גב' אן אפלבאום, ארה"ב
פרופ' ורנון בוגדנור, בריטניה
השופטת דורית ביניש, ישראל
השופט סטיבן ברייר, ארה"ב
השופט סלים ג'ובראן, ישראל
ד"ר איימי גוטמן, ארה"ב
ד"ר ג'וזף ג'ופה, גרמניה
פרופ' רונלד דניאלס, ארה"ב
פרופ' משה הלברטל, ישראל
פרופ' מייקל וולצר, ארה"ב
פרופ' רוברט מנוקין, ארה"ב
פרופ' כריסטוף מרקשיס, גרמניה
השופט אברהם סופר, ארה"ב
מר ברט סטפנס, ארה"ב
פרופ' ארווין קוטלר, קנדה
פרופ' יהודה ריינהרץ, ארה"ב
פרופ' גבריאלה שלו, ישראל

**סגני נשיא**
ד"ר ישי (ג'סי) פרס, אסטרטגיה
פרופ' קרנית פלוג, מחקר
פרופ' יובל שני, מחקר

**עמיתים בכירים**
פרופ' איסמעיל אבו סעד
פרופ' תמר הרמן
פרופ' עמיחי כהן
פרופ' יותם מרגלית
מר אבי ניסנקורן
פרופ' דניאל סטטמן
פרופ' טליה פישר
פרופ' יובל פלדמן
פרופ' מרדכי קרמניצר
פרופ' גדעון רהט
ד"ר תהילה שוורץ אלטשולר
פרופ' איתן ששינסקי

**מייסדים**
ד"ר אריק כרמון
ד"ר ג'ורג' שולץ (1920-2021)

- העברת הטיפול בטכנולוגיות דו שימושיות מאחריות משרד הביטחון לאחריות משרד הכלכלה ושקילת שיקולים יותר רחבים של פגיעה בתעשיית ההיי טק בגלל משברים כאלה;
- חובות צינון על בכירי מערכת הביטחון לשעבר לפני שהם מתחילים לייצג חברות מול משרד הביטחון;
- יצירת מהלך קו-רגולטורי של שילוב פיקוח עם החלת עקרונות אתיקה על התעשייה.

במרחב השני מתברר כי במקום שבו לא קיימת רגולציה מדינתית או בינלאומית שמטרתה להגן על זכויות אדם, תיכנס הרגולציה מצד ענקיות הדיגיטל - באמצעות הגשת תביעות ענק (כמו בין פייסבוק לNSO), סירוב להנפיק בנסדאק (כמו במקרה של חברת סלברייט), האשמות פומביות (כמו האשמת קנדירו על ידי מייקרוסופט על כך שפרצה למערכת חלונות), הפסקת השקעות (כמו במקרה של מייקרוסופט ואניוויז'ן) והגרוע מכל - ניתוק מהפלטפורמות כמו שעשתה אמזון (AWS) לחלק מחשבונות NSO. בהקשר הזה נדרשת חשיבה האם ההגנה על זכויות האדם נדרשת לא רק מצד עצמה אלא כאמצעי הגנה לתעשיית ההייטק, שהיא, כידוע, הקטר הכלכלי של מדינת ישראל.

יש היגיון רב בפיקוח על יצוא בטחוני, גם טכנולוגי, אבל תכליות הפיקוח צריכות להיות בהירות; מרחבי הפיקוח צריכים להפוך להיות מהודקים יותר ולא רחבים מידי כפי שהם היום; ומה שייחשב כטעון פיקוח – צריך להיות נתון לרגולציה פשוטה יותר, שקופה יותר ובהירה יותר.

בנייר ראשוני זה נעמוד על הנקודות המרכזיות שלדעתנו ראוי שוועדת החוץ והביטחון של הכנסת תדון בהן כבר עכשיו, כבסיס לתיקוני חקיקה ולשינויים מוסדיים וארגוניים שיידרשו בהמשך. הנייר מחולק לשני חלקים – **בחלק הראשון נספק רקע על הסוגיה ובחלק השני נציע נקודות לדיון.**

המכון הישראלי לדמוקרטיה

## חלק ראשון: רקע

### 1. מהי המסגרת החוקית שבתוכה פועל הפיקוח על היצוא של טכנולוגיות ביטחוניות?

חוק הפיקוח על יצוא ביטחוני, 2007 תשס"ז מסדיר את הפיקוח של מדינת ישראל על יצוא **ציוד** (מוצרים ותוכנות) ביטחוני, על מתן **שירותים** בטחוניים ועל העברת **ידע** ביטחוני. חוק הפיקוח קובע כי יצוא ביטחוני טעון רישיון מאת הרשות המוסמכת וכי כל פעולת יצוא תתבצע בהתאם לתנאי הרישיון ."יצוא", לצורך העניין, משמעו "העברה אל מחוץ לישראל, לרבות העברה לשטחי האחריות האזרחית הפלסטינית, וכן העברה בישראל לנציגות דיפלומטית או קונסולרית של מדינת חוץ".

**ציוד ביטחוני, כפי שפירטנו לעיל כולל גם ציוד דו שימושי מפוקח, כלומר, ציוד שמופיע ברשימת ואסנאר ואשר נועד לשימוש ביטחוני.**

הרשות המוסמכת ליישום הוראות חוק הפיקוח היא מנכ"ל משרד הביטחון וראש אגף הפיקוח על היצוא בטחוני במשרד הביטחון (אפ"י). לפני שהוקם אפ"י, בשנת 2006, האחריות היתה של האגף לקידום היצוא הבטחוני (סיב"ט), מה שעורר את הביקורת לגבי כך שמדובר בחתול השומר על השמנת – ומעדיף את האינטרס הכלכלי של היצוא על פני מחוייבויות אחרות.

חוק הפיקוח מורה לשר הביטחון למנות ועדות מייעצות אשר ימליצו לרשות המוסמכת על מתן רישיונות, הוא קובע את הרכב חברי הועדה לפי תפקידיהם ודורש כי יהיו מאושרים כבעלי התאמה ביטחונית על פי חוק השב"כ. לפי החוק, חלה אחריות על מי שמבקש לייצא טכנולוגיות ביטחוניות לברר אם יצוא הפריט טעון רישיון. יצוא ביטחוני בהעדר רישיון חושף את היצואן לסנקציות פליליות: שלוש שנות מאסר או קנס ובנסיבות מחמירות חמש שנות מאסר וקנס מוגדל. חוק הפיקוח אינו עוסק רק ביצואן עצמו ומטיל סנקציות פליליות על נושא משרה בתאגיד שהפר את חובתו לפקח ולעשות כל הניתן בכדי למנוע יצוא ביטחוני בהעדר רישיון בידי התאגיד או בידי עובד מעובדיו.

בשנים האחרונות משרד הביטחון יצר הליך אישור מהיר למכירת כלי סייבר התקפי אשר קיצר מאוד את משך הזמן לקבלת רישיון יצוא – משנה לארבעה חודשים. משרד הביטחון גם צמצם את וההגבלות על מערכות אלו, ובעת חברות סייבר התקפי יכולות לקבל פטור מקבלת רישיון לשיווק ולמכירה של מוצרים מסוימים למדינות ספציפיות. מדיניות מקילה זו ספגה ביקורת מהאו"ם ומארגוני זכויות אדם והגנת פרטיות בעולם, הסבורים שעל

מדינת ישראל להגביל את מתן רישיונות היצוא לכלי סייבר התקפי שעלול להיעשות בהם שימוש לרעה לשם הפרת זכויות אדם במדינות דיקטטוריות, כמו סעודיה, סין, סודן, מלזיה ואיחוד האמירויות.[1]

כמו כן, ביוני 2018 הטיל משרד האוצר האמריקאי סנקציות על שתי חברות סייבר ישראליות, Embedi ו-ERPScan, עקב מעורבותן לכאורה בסיוע למתקפות סייבר שביצעה ממשלת רוסיה נגד מוסדות אמריקנים גדולים.[2]

## 2. מה מקומה של מערכת "פגסוס" מבית NSO בתוך "שרשרת ההרג" של מוצרי "סייבר התקפי"[3]?

מקובל לתאר את האופן שבו מתנהלת מתקפת סייבר באמצעות מודל בן שבעה שלבים המכונה "שרשרת ההרג" ("kill chain") שפותח על ידי חברת לוקהיד מרטין כדי לחקור ולהבין את השלבים השונים בתקיפות סייבר. לפי מודל זה מתקפת סייבר מתחילה **באיסוף מודיעין** כאשר התוקף בוחן את מטרת התקיפה ומנסה לאתר חולשות אשר יאפשרו לו לחדור למערכות המותקפות. חולשה היא פִּרצה טכנולוגית או זיהוי התנהגות בלתי צפויה של מערכת המִחשוב המאפשרת לתוקף פוטנציאלי לקבל גישה למערכת או לבצע בה פעולות שלא אמורה להיות לו הרשאה לביצוען. לאחר איסוף המודיעין מתרחש שלב **החימוש** במהלכו התוקף מכין נוזקה (malware), תוכנת מחשב זדונית, המתאימה לחולשה שמצא. השלב השלישי מכונה **הפצה** ובמהלכו התוקף משלח את הנוזקה שפיתח או רכש בשלב השני, בהתאם לאיסוף המודיעין ואיתור החולשות שביצע בשלב הראשון. לאחר מכן מגיע שלב הניצול, לאחריו ההתקנה במהלכה הנוזקה מתקינה את עצמה במערכות המותקפות, שלב השליטה והבקרה במהלכו התוקף מתקין "דלת אחורית" במערכות המותקפות על מנת לשלוט במתקפת הסייבר מרחוק והשלב האחרון שלב הפעולות להשגת מטרת התקיפה.

**ניצול** (exploit) הוא מה שמוגדר כשלב הרביעי בשרשרת. זהו השלב שבו מופעל

---

[1] *Offering Software*; משה גורלי "בלאק קיוב לא לבד" **כלכליסט** (9.6.2019); שוקי טאוסיג "מנוולים, חובבנים ובריונים" **העין השביעית** (7.6.2019).

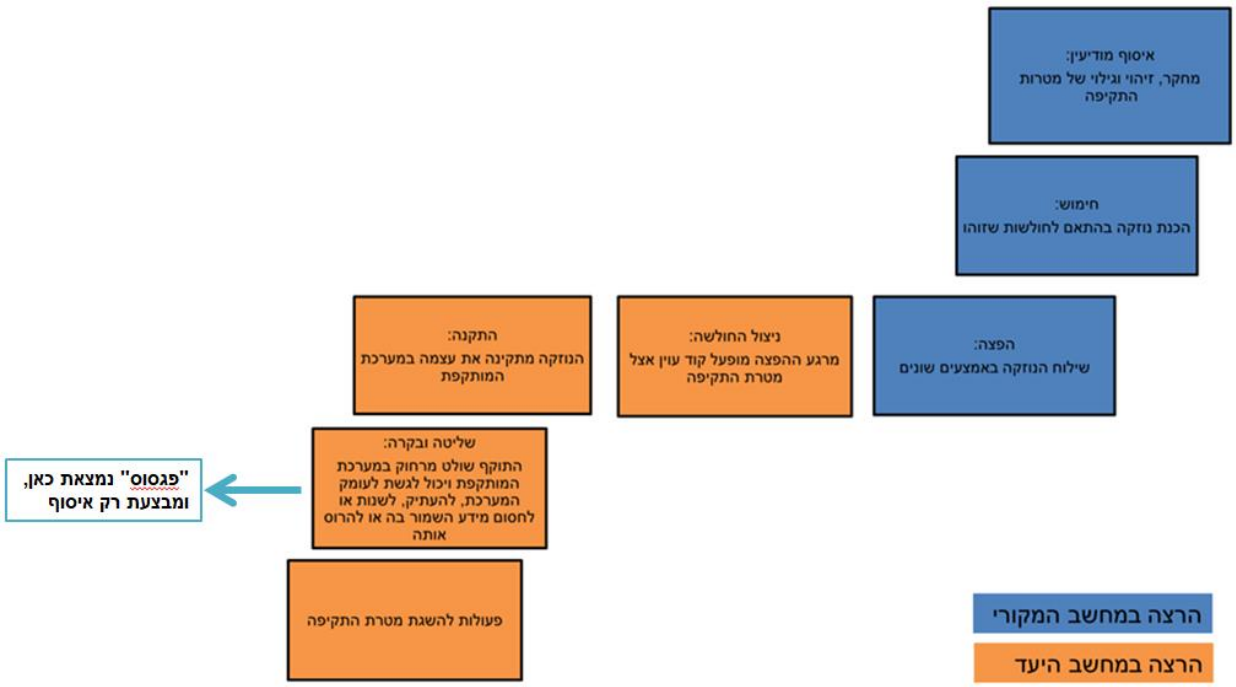
[2] זיו "חברת הסייבר המסתורית"; יוסי הטוני "ישראל מקלה את ההגבלות על יצוא סייבר התקפי – וחוטפת ביקורת" **PC אנשים ומחשבים** (26.8.2019).

[3] להרחבה ראו רחל ארידור הרשקוביץ, תהילה שוורץ אלטשולר ועידו סיוון סיבילה, מה זה סייבר – מושגים ושיטות, ירושלים, המכון הישראלי לדמוקרטיה, 2021.

המכון הישראלי לדמוקרטיה

במחשב המותקף קטע הקוד בנוזקה שנכתב במטרה לנצל את החולשה שהתגלתה בשלב הראשון של איסוף המודיעין, כדי לספק לתוקף הרשאות גישה בלתי מורשות למערכת הממוחשבת שהתוקף מבקש לתקוף.

בגרף הבא נתאר את **"שרשרת ההרג" של הסייבר ההתקפי** ונסביר היכן נמצאת מערכת "פגסוס" בתוך השרשרת:




בשנים האחרונות אנו עדים להפיכת שוק פיתוח הנוזקות לשוק עסקי, שנעשות בו פעולות של הזמנה, אספקה, קנייה ומכירה. בדיוק כפי שאפשר לרכוש תוכנה כשירות (Software as a Service) אפשר לרכוש נוזקה כשירות (Malware as a Service).

למעשה, מפתחי נוזקות הפכו לשכירי חרב המספקים שירותי פיתוח נוזקות, לרבות שירות תמיכת לקוחות וליווי במהלך השימוש בנוזקה. כך, המבקשים לבצע מתקפת סייבר יכולים לבצע למעשה מיקור חוץ של היכולות הטכנולוגיות הדרושות לתקיפה ובכך מתגברים על החסמים הטכנולוגים העומדים בפניהם. נוזקות ומידע על חולשות הניתנות לניצול זמינים להורדה ולרכישה בשירות ברשת האפלה (darknet).[4] בכל שעולם הסייבר מתפתח שירותים

[4] הרשת האפלה, המכונה גם "הרשת השקופה" או "הרשת הנסתרת", מורכבת מאתרי אינטרנט שאינם נגישים באמצעות מנוע חיפוש רגיל דוגמת גוגל. מפעילי האתרים אינם מעוניינים להנגישם לכלל משתמשי האינטרנט בעולם באמצעות מנוע חיפוש, והגישה אליהם נעשית

אלה מגיעים אל העולם ה"אמיתי" וחברות מסחריות ברחבי העולם מציעות שירותי "סייבר התקפי". כמה מהחברות המרכזיות בתחום הן קבוצת גמא, שבבעלות אנגלית-גרמנית; Hacking Team, שבבעלות איטלקית; ו-NSO מישראל.[5] אין מדובר רק בשירותי סייבר התקפי המתמקדים במניעת גישה למערכות ממוחשבות עד לתשלום כופר, פגיעה בתשתיות קריטיות או מתקפה המכוונת לאיסוף פרטי כרטיסי אשראי ומכירתם. **רבות מחברות הסייבר ההתקפי עוסקות באיסוף, ריגול ומעקב באמצעות סוגים שונים של נוזקות ומתקפות סייבר.**

חשוב להבין כי אין מדובר באיסוף המידע השיטתי הנאגם על כל אחד מאיתנו בכל יום ובכל דקה באמצעות יישומונים המותקנים לאחר קבלת רשותנו במכשיר הטלפון הנייד האישי שלנו, כגון רשת חברתית, עוזר דיגיטלי או מנוע חיפוש. אף שמדובר באיסוף מטריד ביותר, הוא נעשה על פי רוב בהסכמתנו, גם אם זו ניתנת באופן אוטומטי ומבלי להבין את השלכותיה עד תום.[6] **איסוף המידע, המעקב והריגול שמבצעות חברות סייבר התקפי נעשה על פי רוב שלא בידיעת נושא המידע, ובוודאי שלא בהסכמתו, באמצעות החדרת נוזקה למכשיר הסלולרי האישי שלו.**

שוק חברות הסייבר ההתקפי משגשג בישראל,[7] ומונה כמה חברות פרטיות אשר פועלות בחשאי והמידע עליהן מועט. על פי רוב הן מגייסות את מרבית עובדיהן מקרב יוצאי יחידות מודיעין מובחרות בתחום לוחמת הסייבר, ובדומה לחברות סייבר התקפי אחרות בעולם, גם אלו הישראליות מוכרות בעיקר אמצעי איסוף, מעקב וריגול.

חברת **NSO**, נחשבת לחברת הסייבר ההתקפי הגדולה בישראל על פי הערכות של היקף פעילותה ומספר העובדים בה. NSO פועלת גם בשוק בישראל, אך היא התפרסמה בעיקר בגין מכירת נשק הסייבר שהיא מפתחת למדינות דיקטטוריות כגון סין, איחוד האמירויות וסעודיה, ולמדינות סמי-דמוקרטיות כמו הודו והונגריה. בשבועות האחרונים, עולות הטענות (שאינן חדשות) כי נשק זה שימש לשם מעקב אחר פעילי זכויות אדם, עיתונאים ומתנגדים למשטר במדינות אלה.

על פי הדיווחים, תוכנת פגסוס (Pegasus) שהחברה פיתחה מאפשרת למשתמש בה לקבל גישה מרחוק למכשיר הטלפון הנייד של מושא המעקב ולאסוף ממנו מידע, לרבות הודעות טקסט, לוג שיחות ונתוני מיקום, תמונות, סרטונים, אנשי קשר ופעילות ביישומונים נוספים כמו רשתות חברתיות.

---

באמצעות תוכנה ייחודית, כמו TOR (The Onion Router) או Comodo dragon browser. ראו רנן אלעל "דארקנט: העולם התחתון של האינטרנט" **ynet** (6.4.2013); JAMIE BARTLETT, THE DARK NET: INSIDE THE DIGITAL UNDERWORLD (2016)

[5] *Offering Software for Snooping to Governments is a Booming Business*, THE ECONOMIST (Dec. 14, 2019) (להלן: *Offering Software*)

[6] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019)

[7] *Offering Software*, **לעיל**.

המכון הישראלי לדמוקרטיה

לדברי החברה: (1) היא משווקת את מוצריה לממשלות, רשויות אכיפת חוק וסוכנויות מודיעין מדינתיות בלבד.[8] (2) החברה איננה פוגעת במחשב או בטלפון הנייד שאליו היא פורצת, היא לא משתקת את הגישה אליו או מוחקת או עורכת כל מניפולציה אחרת במידע, אלא רק אוספת ומעתיקה את המידע. (3) היא לא מפעילה את המוצר ולא מנטרת את הפעלתו בזמן אמת, אלא משאירה לעצמה את האפשרות לדרוש לבדוק אותו בדיעבד על בסיס מידע המצביע על אפשרות לשימוש לרעה.

יודגש, כי NSO אינה החברה היחידה שמבצעת פעולות כגון אלה.

"**בלאק קיוב**", שהוקמה על ידי יוצאי קהילת המודיעין הישראלית למטרות מודיעין עסקי, ומשלבת שירותי סייבר התקפי לצד יכולות מודיעיניות מוכרות מתחום המודיעין האנושי (יומינט) ומודיעין האותות (סיגינט). החברה מספקת שירותי תמיכה בליטיגציה משפטית, איסוף מודיעין עסקי וראיות, ייעוץ אסטרטגי בסכסוכים משפטיים, מתן מודיעין לאיתור נכסים וזיהוי סימני שחיתות או ניגוד עניינים. סוכני החברה מסוגלים לאסוף מידע ולעקוב אחר מטרותיהם באמצעות גישה לחשבונות בנק, דוחות כרטיסי אשראי, ניטור חשבונות הרשתות החברתיות של מושא המעקב וחבריו ומעקב אחר נתוני המיקום של מכשיר הטלפון הנייד שלו. באפריל 2017 נעצרו שני עובדי החברה בחדר מלון ברומניה, ונטען כי ניסו להשיג דגימות DNA של ראש הרשות למלחמה בשחיתות ברומניה ואף ביצעו תקיפת סייבר נגדה באמצעות פריצה לחשבונות דוא"ל של כמה ממקורביה. בהמשך הסתבכה החברה בניסיון לברר את מניעיה של המתלוננת הראשונה שטענה כי המפיק והבמאי האמריקאי הרווי ויינסטיין אנס אותה.[9]

חברת **קנדירו**, הנחשבת השנייה בגודלה בשוק הסייבר ההתקפי בישראל, מספקת, לפי דיווחים בתקשורת, מערכת מלאה למתקפת סייבר הכוללת סל של שירותים: זיהוי חולשה, ממשק משתמש שמאפשר ללקוח לראות כמה יעדים נחדרו ואיזה מידע הושג ומגוון נוזקות, ואף פיתוח נוזקות חדשות אם אלה הקיימות במערכת אינן מספיקות. למשל, קנדירו מספקת פלטפורמה שאינה ניתנת לאיתור המשמשת לחדירה למערכות מחשב, לרשתות ולמכשירי טלפון ניידים. בין השאר, המערכת מאפשרת למשתמש בה לשלוט מרחוק ולבצע מניפולציות במיקרופון, במצלמה ובמקלדת של מכשיר הטלפון הנייד, ואף לצלם צילומי מסך, להאזין לשיחות VoIP

---

[8] Ronan Farrow, *The Black Cube Chronicles: The Double Agent*, THE NEW YORKER (Oct. 9, 2019); Ben Gilbert, *Meet the Shadowy Security Firm from Israel Whose Technology is Believed to be at the Heart of the Massive WhatsApp Hack*, BUSINESS INSIDER (May 14, 2019)

[9] יואב סטולר ואור הירשאוגה "חברת הסייבר המסתורית בשירות משרד הביטחון" **כלכליסט** (29.3.2018); יובל הירשהורן "בתוך הקופסה השחורה" **פורבס** (8.11.2017); Ronen Bergman & Scott Shane, *The Case of the Bumbling Spy: A Watchdog Group Gets Him on Camera*, THE NEW YORK TIMES (Jan. 28, 2019); Ronan Farrow, *The Black Cube Chronicles: The Private Investigators*, THE NEW YORKER (Oct. 7, 2019)

ולצותת לתוכנות מסרים מיידיים. קנדירו משווקת את מוצריה לממשלות בכל רחבי העולם, למעט בישראל, ארה"ב, רוסיה וסין.[10]

חברת **PICSIX** עוסקת אף היא, לפי הדיווחים בתקשורת, בסייבר התקפי ובעיקר במעקב והאזנה ברשתות סלולר. גם חברות ישראליות נוספות, **כגון Rayzonre, Wintego, Septier, ורינט ואלביט מערכות**, עוסקות בסייבר התקפי.[11]

## 3. מהי טכנולוגיה "דו שימושית"?

תוכנת מעקב כגון "פגסוס" של חברת NSO מאפשרת למחזיק בה להשתלט מרחוק על טלפון נייד, ולהקליט תמונה וקול באמצעות מנגנוני ההקלטה שבו. בדרך זו הופכת תוכנת המעקב את מכשיר הטלפון הנייד למכשיר ציתות וריגול אקטיבי. אבל, לאמיתו של דבר טכנולוגיות מעקב מיועדות בעיקרן למטרות כשרות ורצויות כמו לחימה בטרור ואכיפת חוק ונמכרות רק לממשלות. NSO, למשל, אף אימצה מדיניות המבוססת על העקרונות המנחים של האו"ם לעסקים ולזכויות אדם, ואוסרת בתנאי השימוש שלה שימוש בתוכנה שבפיתוחה העלול לפגוע בזכויות אדם מסוימות, כגון הזכות לחיים ולביטחון אישי.[12] אולם בפועל, לאחר המכירה של כלים לזיהוי ולניצול חולשה במערכת ממוחשבת או מתן רישיון לשימוש בהם יכול להיעשות בהם גם שימוש לרעה, בעיקר כאשר הם נמכרים לחברות שערכי הדמוקרטיה וזכויות האדם אינם בראש סדר העדיפויות שלהן.[13]

טכנולוגיות שיש להן שימושים אזרחיים אך בה בעת גם שימושים צבאיים, נקראות **טכנולוגיות דו שימושיות** (Dual Use Technologies). בעשורים האחרונים השתרשה בעולם התפיסה שיש לאסדר ולפקח על הפיתוח, ההפצה והייצוא של טכנולוגיות דו שימושיות כאשר השימוש הצבאי בהן יכול להוות סכנה לשלום העולמי ומנוגד לכללי המלחמה הבינלאומיים.

בשל כך **בהסדר ואסנאר**[14], שהוא הסדר בינלאומי משנת 1996 שמיועד להבטחת

---

[10] אמיתי זיו "'גאווה' כחול לבן: חברת הסייבר קנדירו משווקת כלי פריצה לטלפונים סלולריים" **TheMarker** (2.9.2020); Thomas Brewster, *Mysterious Mercenaries Hacking Apple and Microsoft PCs For Profit*, FORBES (Oct. 3, 2019)

[11] אמיתי זיו "חברת הסייבר המסתורית שמשלמת להאקרים שלה 80 אלף שקל בחודש" **TheMarker** (3.1.2019) (להלן: זיו "חברת הסייבר המסתורית").

[12] *Offering Software* ,**לעיל**; William Turton & Davide Scigliuzzo, *Facebook Sues Israel's NSO on Alleged WhatsApp Malware Hack*, BLOOMBERG (Oct. 29, 2019)

[13] עומר כביר "חברות סייבר התקפי מקלות על האקרים ופושעים לפרוץ לנו לחיים ולשבש אותם" **כלכליסט** (1.9.2019).

[14] The Wassenaar Arrangement on Export Controls of Conventional Arms and Dual Use Goods and Technologies, Participating States, (Jan. 20, 2016), http://www.wassenaar.org/participating-states/.

היציבות הבינלאומית ושעוסק בפיקוח על סחר ויצוא של אמצעי לחימה קונבנציונליים למדינות סוכנות וארגוני טרור, נכללה הקטגוריה של "ציוד דו -שימושי".

עם זאת, מכיוון שקבלת תנאי ואסנאר מאפשרת הסרת חסמים בסחר באמצעים דו -שימושיים, מדינת ישראל מצייתת, באמצעות חקיקה פנימית – חוק הפיקוח על יצוא בטחוני[15], לרשימת הציוד הכלולה בהסכם ולכן זוכה למעמד "מדינה נאמנה" (adherent state) ביחס להסכם. רשימת הטובין והטכנולוגיות הדו -שימושיים מתעדכנת בהסדר ואסנאר מידי שנה בחודש דצמבר. לפי חוק הפיקוח על יצוא בטחוני הקובע כי "ציוד דו-שימושי מפוקח" הוא "ציוד דו-שימושי הכלול ברשימת טובין וטכנולוגיות דו-שימושיים שנקבעה בידי הסדר ואסנאר, כעדכונה מזמן לזמן" – הרשימה המעודכנת מוחלת **אוטומטית** לתוך החוק מידי שנה.

## 4. האם לחברות כמו NSO יש אחריות על פעולות שצד שלישי עושה במערכת שלהן?

כפי שעולה מהפרסומים בימים האחרונים, אחת הטענות היא שלא ניתן להשית אחריות על NSO ודומותיה, כאשר מי שרכש מהן את המוצר ואף התחייב לעשות בו שימוש למטרות ראויות, עושה במערכת שימוש לרעה ומבצע מעקבים אחר עיתונאים, ראשי מדינות, פעילי זכויות אדם ועוד, מה שמכשיר אחר כך את הקרקע לפגיעה פיסית באותם נעקבים.

למשמע טענות אלו קשה שלא להיזכר בסוגיה המשפטית שעלתה בשנות התשעים, בראשית ימיו של האינטרנט לגבי מכשירי הוידאו של סוני ולגבי בתוכנות שיתוף הקבצים נאפסטר וגרוקסטר, שהשתמשו בהם כדי להעתיק תכני טלוויזיה וליצור שוק שחור עולמי ענק של תכנים אלה. גם שם נטען שהפגיעה בזכויות היוצרים אינה מבוצעת בפועל על ידי החברה המפתחת את הטכנולוגיה, אלא על ידי מי שקיבל ממנה רישיון שימוש.

לקראת סוף שנות התשעים התפתחו מכשירים משפטיים לצורך הגנת יצירות המוגנות בזכות יוצרים סביב מכשירי הוידאו ותוכנות שיתוף הקבצים כדי לפתור את הבעיה והוחלה "אחריות תורמת" על מפתחי הטכנולוגיה. **כעת, נדרשת חשיבת רוחב בעולם וגם ובישראל על יבוא דוקטרינת ההפרה התורמת גם לדיון המשפטי באחריות חברה המפתחת טכנולוגיות מעקב, לשימוש שנעשה בטכנולוגיות שפיתחה.**

---

The Wassenaar Arrangement on Export Controls of Conventional Arms and Dual Use Goods and Technologies, Best Practices for Effective Enforcement, (Dec. 1, 2000), http://www.wassenaar.org/best-practices-for-effective-enforcement/.

[15] **חוק הפיקוח על יצוא בטחוני , תשס"ז 2007.**

המכון הישראלי לדמוקרטיה

## חלק ב: נקודות לדיון

### 1. השיקולים שיש לשקול בהליך מתן הרישיונות במסגרת חוק הפיקוח

חוק הפיקוח על היצוא הביטחוני קובע, בפשטות, כי תכליות הפיקוח הן שמירה על הביטחון הלאומי, יחסי החוץ של המדינה ו"אינטרסים חיוניים" אחרים של המדינה. החוק אינו מזכיר שיקולים של השלכות הסחר בנשק סייבר התקפי על זכויות אדם במדינות אחרות. החוק אינו עוסק גם בזכויות אחרות כגון זכויות העיסוק והקניין של היצואנים; שיקולים כלל משקיים כגון צמצום היקף ההשקעות בתעשיית הסייבר הישראלית ופגיעה בכושר התחרות של חברות מקומיות בשוק הגלובלי. הסיבה המרכזית לכך היא שחקיקת החוק והקמת אפ"י לא נבעו מרצון להגן על זכויות האדם, אלא נבעו ישירות מדרישה אמריקנית בעקבות פרשת מטוס הפלקון שעסקה ביצוא טכנולוגיות של התעשיה האווירית לסין ויצרה משבר ביחסי ישראל ארצות הברית.

אכן, לאורך השנים השיקולים שנשקלים בהכרעות לגבי אישור על ייצוא טכנולוגיות בטחוניות הם שיקולי ביטחון (שהנשק לא יגיע בטעות לחיזבאללה) ושיקולי יחסים בין לאומיים של מדינת ישראל שבהם נכללים שיקולי מלחמות סחר (למי אפשר למכור בלי להרגיז את האמריקנים), שיקולי יחסי חוץ של מדינת ישראל (למי נעניק את "פגסוס" כמתנת ידידות) ושיקולים גיאו אסטרטגיים (לאיזו מדינה מזרח תיכונית נמכור את המערכת כדי שתשתיק מהומות ותקדם שקט באזורנו).

מנגד, אחת מתכליות הפיקוח הבינלאומי על יצוא ציוד דו- שימושי היא מניעת זליגת הטכנולוגיה לידיהם של משטרים אשר אינם מכבדים עקרונות בסיסיים של זכויות אדם. לכן, לתפיסת המדינות החברות בהסדר ואסנאר מטרת הפיקוח היא לצמצם את הסיכוי שמוצרי ריגול ומעקב, יגיעו לארגוני טרור או למשטרים טוטליטריים העלולים לעשות שימוש בכלים אלו לשם פגיעה במי שהם תופסים כמתנגדי המשטר. יתרה מזאת, בחמש השנים האחרונות יש טענות קשות כלפי ישראל על כך שהיא שותפה בפגיעה בזכויות אדם בשל יצוא טכנולוגיות ריגול ומעקב וכי עליה לשנות את משטר הפיקוח שלה.

בנוסף, פעילי זכויות אדם כגון עו"ד איתי מק וארגונים כגון אמנסטי מגישים עתירות כנגד מנכ"ל משרד הביטחון וראשי אפ"י בשל אישורים שניתנים למכירת טכנולוגיות למדינות לא דמוקרטיות. פעולות אלה גורמות לכך שנלקח

לפעמים בחשבון השיקול של זכויות אדם, רק כדי להימנע מן הדיון בערכאות אף שהדיונים האלה כשלעצמם מתנהלים מאחורי דלתיים סגורות והמדינה מציגה שם לבית המשפט חומר חסוי בלבד.

הבעיה היא שאך לפני כמה שבועות קבע בג"ץ - בעתירה שהגישו פעילי זכויות אדם נגד משרד הביטחון ובה ביקשו לא לאשר ייצוא של מערכות לפריצת טלפונים של חברת סלברייט לגוף שכפוף לנשיא רוסיה – כי לא יפעיל ביקורת שיפוטית אלא במקרים חריגים ביותר. "כבשאר העניינים של יחסי חוץ וביטחון", כתבו השופטים אלכס שטיין, ענת ברון ודוד מינץ, "שיקול הדעת המצוי בידי רשויות המדינה הינו רחב במיוחד"[16]. כלומר, העובדה שבג"ץ איננו מתערב בסוגיות השיקולים והמידתיות של החלטות בנושאים אלה, יחד עם חוסר השקיפות, מהווים תמריץ שלילי לאפי"י לשקול שיקולים של זכויות אדם.

**נקודה לדיון: המשבר בעניין NSO מלמד שאי אפשר להמשיך עם מסגרת השיקולים הצרה וחייבים לשקול שיקולי זכויות אדם. הן כי זה ראוי ונכון, והן כי משברים כאלה פוגעים בכלל התעשיה. יש לשקול להוסיף אותם לחקיקה עצמה ומכל מקום חובה לתת להם משקל משמעותי בהחלטות עתידיות.**

## 2. סיבוכיות, דלת מסתובבת ושקיפות בפיקוח על יצוא בטחוני

א. **רגולציה מסובכת** היא אחד המתכונים הישירים לכישלון ולהשחתה של מערך הפיקוח על היצוא הבטחוני. לפי חוק הפיקוח כדי לייצא טכנולוגיות ביטחוניות צריך לעבור הליך של ארבעה שלבים: קבלת רשיון יצואן בטחוני; קבלת רשיון מוצר וסיווג בטחוני למוצר; קבלת רשיון שיווק (כלומר רישיון לנהל משא ומתן עם מדינה כלשהי לגבי המוצר); קבלת רשיון מכירה.

[16] בג"צ 1942/21 יעל אגמון נ. מנכל משרד הביטחון.

בנוסף, כפי שנכתב לעיל, בהקשרים של טכנולוגיות דו שימושיות מאמצת מדינת ישראל כל שנה באופן אוטומטי רשימה המתקבלת מכוח מה שמכונה "הסכם ואסנאר", ונדרש ידע מדעי עצום כדי להבין אותה. זוהי הסיבה שבגללה הקים אחד מיוצאי אפ"י חברה המספקת מנוע חיפוש לרשימה של ואסנאר. נעיר כי אף מדינה מערבית אחרת – ובכלל זה ארצות הברית והאיחוד האירופי – אינה מאמצת את הרשימה באופן אוטומטי ומיידי. החשש הוא שגם במשרד הביטחון מתקשים להסביר מה משתנה ברשימה כל שנה.

רמת סיבוכיות גבוהה יוצרת זירה שנתונה רק בידי מומחי תוכן מועטים, שכולם משמשים בתפקידי ייצוג של לקוחות ומגשרים בינם לבין משרד הביטחון. מומחים אחרים, עיתונאים ובוודאי הציבור הרחב, אינם מסוגלים לקחת חלק במשחק.

**נקודה לדיון: נדרשת התמקדות במה שאכן הכרחי לפקח עליו, ונכון להניח לרשויות אחרות לעסוק במה שאין הכרח שמשרד הביטחון יעסוק בו. מה שיישאר בתוך משרד הביטחון צריך לעבור תהליך של פישוט התהליך. יש לשנות את ההסדר לגבי אימוץ אוטומטי של רשימת ואסאנאר ולשקול אימוץ לאחר תהליך בדיקה.**

ב. **התופעה של "מעבר בטוח"** מגופי רגולציה בטחוניים וממערכת הביטחון בכלל, לייצוג חברות פרטיות מול מערכת הביטחון היא תופעה מוכרת אבל בעייתית. למשל, בהקשר של NSO (וכדוגמה בלבד משום שהיא לגמרי לא לבד) היועץ הבכיר שלה הוא בוקי כרמלי, מי שהקים את מערך הסייבר, עמד בראש המלמ"ב וגם השתתף בדיונים הראשונים מהצד של משרד הביטחון כשהטכנולוגיות של NSO הובאו לדיון. בהנהלת NSO יושבת תא"ל (במיל) אריאלה בן אברהם ששימשה קודם לכן הצנזורית הצבאית הראשית.

כאשר מי שמייצג את היצואניות הם בכירי מערכת הביטחון לשעבר שלהם הרגולטורים הנוכחיים רוחשים כבוד; ואולי גם במוחם של הנוכחיים חולף בדל מחשבה שירצו לעבוד (בשכר גבוה מאד) באחת החברות לאחר שיפרשו, מערך כולו נמצא בבעיה. זאת, מבלי לשאול מה קורה למערכת הביטחון עצמה בגלל ה"מעבר הבטוח" של בכיריה לייצג את חברות הטכנולוגיה. נדגיש כי בהקשר של הפיקוח על יצוא בטחוני מעורבים, מעבר לאגף לפיקוח על יצוא בטחוני (אפ"י), גם האגף לסיוע בטחוני (סיב"ט) שאמור לעודד תעשיות ביטחוניות; האגף הביטחוני –מדיני; המינהל למחקר,

פיתוח אמצעי לחימה ותשתית טכנולוגית (מפא"ת); אגף היועץ המשפטי למערכת הביטחון; ויחידת הממונה על הביטחון במערכת הביטחון (מלמ"ב). המעורבות של כל הגופים האלה מרחיבה מאד את יכולת ההשפעה של בכירים לשעבר במערכת הביטחון ובצבא עליהם.

בשנות ה-90 הנהירה של בכירים באוצר וברשויות רגולטוריות אל שוקי התקשורת והתשתיות הובילה להבנה שמתרחשת תופעה של "רגולטור שבוי", ושעצם אפשרות המעבר אל התעשייה משפיעה על תהליכי קבלת החלטות בתוך הרשויות. הייתכן שדבר כזה מתרחש גם בתוך מערכת הביטחון, אבל אנחנו לא יודעים?

**נקודה לדיון: ניקוי התופעה של "יד רוחצת יד" הוא תנאי מוקדם לטיוב הרגולציה; יש לשקול חובות צינון על הופעה בפני מערכת הביטחון כשמדובר ברגולטורים או בנושא דרגות בכירות במיוחד בצבא ובמערכת הביטחון.**

ג. הפיקוח על הייצוא הבטחוני נעשה **מאחורי מסך** של היעדר כפיפות לחוק חופש המידע ואפילו תוך שימוש בצנזורה הצבאית. כל פניה מצד עיתונאים נענית בתשובה לקונית שלפיה משרד הביטחון אינו מוסר פרטים אודות מדיניות הייצוא הבטחוני ובכלל זה אינו מתייחס לרשיונות ספציפיים או לרשומים במרשם הייצוא, וזאת מטעמים ביטחוניים, מדיניים ואסטרטגיים. גם דיונים בבתי משפט מתבצעים בדלתיים סגורות וחומרים מוצגים בפני השופטים תחת חיסיון בטחוני. כך, לא ניתן לדעת אילו טכנולוגיות המערכת מאשרת למכור, ולמי; מהם השיקולים שנשקלים; מתי החברות משרתות את המדינה ומתי את עצמן, ומי קובע זאת. גם העירוב בין עבודה עבור מערכת הביטחון וקשרי עבר איתה - נעשה מאחורי מסך זה.

**נקודה לדיון: שקיפות היא ערך מרכזי בסוגיות של רגולציה. יש לפעול להסרת מסך ההסתרה מאחורי התעשיה של ייצוא טכנולוגיות ביטחוניות לטובת כללי סודיות מאוזנים יותר. כללים אלה צריכים לכלול את רשימת היצואנים; רשימת נושאי המשרה וחברי הדירקטוריונים שלהם; רשימת המוצרים שאין עליהם סיווג בטחוני; מספר הבקשות שהוגשו ומספר רישיונות הייצוא שניתנו בחתך של בעלי רישיון יצואן.**

**ברור לנו לא תהיה שקיפות מלאה בעולמות האלה, והדבר מובן ומוצדק, אבל המצב הנוכחי נוח מידי לשחקנים ורע לאינטרס הציבורי.**

## 3. המיקום הארגוני של פיקוח על יצוא מוצרים דו שימושיים

כשם שמטרות שונות של רגולציה עומדות לפעמים בסתירה זו לזו, כך גם הרשויות הרגולטוריות שמיישמות אותה. יותר רשויות משמען יותר מתחים, קונפליקטים ומלחמות טריטוריה רגולטוריות. כאמור, בהקשר של הפיקוח על יצוא בטחוני קיימים גופים שונים בתוך משרד הביטחון ובראשם סיב"ט ואפ"י. בחוק הפיקוח יש חובה לכלול בוועדות נציגי משרד החוץ ונתונה גם להם זכות וטו. כך, למשל, בעקבות האירועים של רצח העם במיאנמר בוטלו הרישיונות לייצוא לשם.

בנוסף, במשרד הכלכלה קיים אגף הפיקוח על הייצוא, המפקח על מכירת טכנולוגיות דו שימושיות לגופים אזרחיים, מכוח פקודה מנדטורית - מכוח פקודת המסחר עם האויב, 1939. כך, בעוד שמשרד הביטחון מפקח על מכירה למדינות, ועל כל דבר שיש לו היבט קצה בטחוני, כולל מכירה לגורמי אכיפת חוק (משטרה וכיו"ב), מפקח משרד הכלכלה על שאר המוצרים הדו שימושיים – אלה שמיועדים למשתמשים אזרחיים. בכל העולם המערבי הייצוא הצבאי מפוקח על ידי רשויות ביטחון בעוד שהייצוא הדו שימושי מפוקח על ידי רשויות תעשיה ומסחר אזרחיות, הואיל ומדובר בציוד שהומצא לכתחילה עבור מרחב אזרחי. בזמן חקיקת חוק הפיקוח, לא הסכים משרד הביטחון שהפיקוח יעבור לאחריות משרד הכלכלה (אז התמ"ת). היקף האיסור שמטילה הפקודה הינו נרחב מאוד וכולל בפועל כל סוג של פעילות כלכלית עם אויב או לטובתו. במשרד הכלכלה הוקם אגף הפיקוח על הייצוא אבל הוא משמש בעיקר לנקודת מעבר לנספחים הכלכליים בין שליחות לשליחות וחסר יציבות ארגונית. לאגף הפיקוח במשרד הכלכלה אין יכולת אכיפה (אם לא פונים אליהם לקבל רישיון הם לא יכולים לעשות כלום), הפרת החוק היא עבירה פלילית אבל אין כלים

מנהליים והדבר יוצר כשל אכיפה. משרד הכלכלה ניסה לחזק את סמכויות האכיפה שלו באמצעות עירוב גוף נוסף – "וועדת כופר" להטלת קנסות על מי שמייצא שלא כדין, דרך חוק המכס.

גם מערך הסייבר הלאומי הוציא בשנת 2015 צו שבו הוא רוצה לקחת לעצמו סמכויות פיקוח על מוצרי סייבר שנוגעים לתשתיות קריטיות, מה שגרם למתח בינו לבין אפ"י.

**נקודה לדיון: יש צורך בגבולות גזרה בהירים בין הגופים ובהעברת הפיקוח על מוצרים דו שימושיים למשרד הכלכלה.**

**נדרש חוק חדש במקום פקודת המסחר עם האוייב משנת 1939 שיעביר את הפיקוח על כל רשימת הציוד הדו שימוש לאגף הפיקוח על הייצוא במשרד הכלכלה ויותיר למשרד הביטחון לעסוק בציוד לחימה ובטילים. החוק יקבע מסגרת רחבה של שיקולים וביניהם שיקולי זכויות אדם, מעבר לשיקולי הביטחון והחוץ; יחזק את סמכויות האכיפה של אגף הפיקוח במשרד הכלכלה ויוסיף גם סמכויות אכיפה מנהליות; יקבע עבור התהליך כללי שקיפות מאוזנים וברורים; יחייב הנמקה במתן או שלילת רישיונות; ויחזק את המבנה הארגוני של אגף הפיקוח ואת התקציב שלו. נציגי משרדי הביטחון והחוץ יהיו חברים בוועדות הרישוי.**

**לא רצוי להעביר את סמכויות אפ"י בנוגע לטכנולוגיות דו שימושיות למערך הסייבר הלאומי, בשל הפטור ממחוייבותו לשקיפות בהיותו גוף בטחוני והיעדר סמכויות רגולטוריות אזרחיות אחרות, עד שייחקק חוק סייבר.**

**אם יושאר הפיקוח בידי משרד הביטחון יש ליצור הפרדה בין הזרוע המסייעת ליצוא בטחוני (סיב"ט) ובין הזרוע המפקחת (אפ"י) ולקדם עקרונות של שקיפות ורישום כפי שנכתב למעלה.**

המכון הישראלי
לדמוקרטיה

## 4. היחס בין אסדרה כופה ושיקולי אתיקה

רגולציה טובה היא כזאת שכוללת ציווי ושליטה וגם אמצעים רכים יותר ובתוכם עידוד לרגולציה עצמית. במקרה של פיקוח על יצוא בטחוני, צריכים לדור בכפיפה אחת הרגולציה והאתיקה. השאלה היא קשה: מהם השיקולים ה"קשים" והאתיים שנכון לשקול כשמוכרים מוצר עם פוטנציאל לשימוש לרעה. הדילמה למי למכור ולמי לא למכור טכנולוגיה מסויימת היא גם של המדינה וגם של החברות עצמן: יש מי שרוצה להרוויח בכל מחיר ויש מי שחושש מפגיעה במוניטין או פשוט רוצה לישון טוב בלילה. כיום, היחס בין רגולציה לאתיקה כל כך מגוחך, שנשמעים סיפורים על כך שחברה שיש לה "מנגנון אתיקה" החליטה לא למכור מוצר למדינה מסויימת בגלל שיקולי אתיקה. משרד הביטחון גילה שהחברה לא מוכרת לאותה מדינה ובעס: קיבלתם רישיון שיווק, למה לא מכרתם?

פרופ' דייויד קיי, הדווח המיוחד של מועצת זכויות האדם של האו"ם, האשים כמה פעמים את ישראל בכך שמשטר הפיקוח שלה איננו מהודק ואיננו שקוף; הוא גם האשים את חברת NSO עצמה בכך שאף שהיא מצהירה על מחוייבותה כלפי ה- Guiding Principles on Business and Human Rights של האו"ם, היא איננה מאפשרת לבדוק זאת בפועל. בטור דיעה שהתפרסם בוושינגטון פוסט לפני כמה ימים, חזר קיי על טענה זאת[17]. NSO פרסמה "דו"ח אתיקה" ביוני 2021, ואולם ביקורת נמתחה על כך שגם בדו"ח האתיקה לא נמצאו פרטים מספקים[18].

---

[17] David Kaye and Marietje Schaake, Global spyware such as Pegasus is a threat to democracy. Here's how to stop it, Washington Post, 19.7.2021 https://www.washingtonpost.com/opinions/2021/07/19/pegasus-spyware-nso-group-threat-democracy-journalism/.

[18] ראו למשל, עומר כביר, כלכליסט, 31.6.2021 https://www.calcalist.co.il/technology/article/SJMmNM52u

המכון הישראלי
לדמוקרטיה

**נקודה לדיון: גישה רגולטורית נכונה צריכה ליצור מסגרת מקובלת של שיקולי אתיקה בהידברות עם התעשייה. למשל, שיקולים כגון אלה שמופיעים בהמלצות דו"ח קיי או בקריטריונים של ארגון CAUSE – Coalition Against Unlawful Surveillance Export – ל"בדיקת נאותות אתית" של המדינה הרוכשת כאשר מתעורר חשש לגבי כוונותיה.**

**למשל, עמידה של מדינת היעד בחובות המעוגנות באמנות לזכויות אדם; מצב זכויות האדם של אזרחי המדינה הרוכשת; עמידה בקריטריונים של קוד ההתנהגות של האיחוד האירופי ליצוא טכנולוגיות צבאיות; וקיומה של מסגרת משפטית רלוונטית במדינת או ארגון היעד שתבטיח שהשימוש בטכנולוגיה לא יעשה באופן הפוגע בזכויות אדם.**

## 5. הרגולציה על ידי ענקיות האינטרנט והשלכותיה

יומיים אחרי שהתפוצצה פרשת פגסוס, אישרה חברת אמזון ( AWS) שהיא ניתקה חשבונות בענן שהיו מקושרים לקבוצת NSO. מה שככל הנראה הרגיז את אמזון, הוא העובדה שנעשה שימוש בפלטפורמת CloudFront, אחד משירותי הענן שהיא מספקת – רשת העברת תכנים (CDN) המאפשרת ללקוחות להעביר דאטה, וידאו, אפליקציות ו - APIs באופן מהיר ובטוח - כדי להעביר את השלבים הראשונים של המתקפות כנגד המכשירים הניידים (שאליהם פרצה NSO) וכדי להסתיר את פעילות המעקב. כאשר ארגון "אמנסטי אינטרנשונל" פנה לאמזון בעניין, הודיע דובר מטעם אמזון לרשת CNN כי הם פעלו מהר כדי לכבות את החשבונות והרשת הרלבנטיים.

**מה שהדובר לא הודיע הוא מכוח איזו מדיניות או איזה סעיף בתנאי השימוש של AWS חסמה אמזון את החשבונות של NSO.** הרי כשאמזון איפשרה ל NSO לרכוש ממנה שירותים בשנים האחרונות, לא היתה בעיה. יותר מזה, במאי 2020, כאשר אתר vice פרסם חשדות ש- NSO עשתה שימוש בתשתית של אמזון כדי להעביר נוזקות, אמזון אפילו לא הגיבה לפניות עיתונאים.

פעילות זו דומה ל"דה-פלטפורמינג" שביצעו ענקיות הדיגיטל בדונאלד טראמפ אחרי הפריצה לקפיטול בינואר 2021.

סגירת חשבונות NSO יחד עם המקרה של הורדת הרשת החברתית "פרלר" בינואר 2021, וגם שיתוק חשבונות ארגון

וויקיליקס בשנת 2010, מלמדים שאמזון לא מהססת לעשות די-פלטפורמינג כשמדובר בהפרות "פוליטיות" של תנאי השימוש: הפרת זכויות אדם והבכת בכירי הממשל בעולם. בעולם הנוכחי, במקום שבו רגולציה מדינתית או בינלאומית כדי להגן על זכויות האדם לא עובדת, תיכנס הרגולציה מצד ענקיות הדיגיטל – באמצעות ניתוק מהפלטפורמות. במאי השנה, סביב מבצע "שומר החומות" בעזה, התפרסם באתר הטכנולוגיה The verge שיותר מחמש מאות עובדי אמזון חתמו על מכתב שבו הם קוראים למנכ"ל החברה ג'ף בזוס ולמנכ"ל שירותי הענן של אמזון אנדי ג'סי להכיר בסבל של הפלסטינים ולבטל חוזים עם ממשלת ישראל. מה יקרה כשהלחץ הזה יעבוד או כשיתפרסמו עוד סיפורים דוגמת זה של NSO?

**נקודה לדיון: האם כאשר מדינת ישראל מפקידה באופן ריכוזי את כל הנכסים הדיגיטליים שלה, כולל אלה של משרד הביטחון וצה"ל, בידי אמזון, במסגרת פרוייקט "נימבוס" היא מערכת לכך שהסטנדרטים של אמזון יהפכו לריבון האמיתי שלנו ויהיו חשובים יותר מכל חקיקה מדינתית, וששיקוליה של אמזון לא יהיו תמיד גלויים ובהירים ולכן חשבונות המקושרים לארגוני בטחון או חברות ישראליות עשויים למצוא את עצמם מחוץ לענן במקרה של חשדות להפרת זכויות אדם.**

## 6. אנחנו במסלול התנגשות מול אירופה והאו"ם

המכון הישראלי לדמוקרטיה

לפני כמה חודשים יזם האיחוד האירופי תיקון חקיקה בנושא של פיקוח על יצוא של מוצרים דו שימושי בדגש על מוצרי ריגול ואיסוף. תיקון החקיקה שאושר בפרלמנט האירופי ייכנס לתוקף בספטמבר. התיקון מקשיח את כללי הפיקוח על הייצוא, מעלה את החשיבות של פגיעה בזכויות אדם כשיקול למתן רישיונות ומגדיל את טווח האפשרויות לפיקוח על ייצוא בתוך היבשת.

**סיכום של החקיקה האירופית נמצא בנספח א.**

ביולי 2019 פורסם דו"ח מפורט[19] הכולל המלצות על ידי פרופ' דייויד קיי, הדווח המיוחד לענייני חופש ביטוי של מועצת זכויות האדם של האו"ם בנוגע לפיקוח על יצוא טכנולוגיות מעקב. ההמלצות הנוגעות למדינות כוללות הצעה להטיל מורטוריום מיידי על מדינות לייצא, למכור, להעביר ולהשתמש בכלי מעקב עד שייקבע משטר בינלאומי בנוגע למסחר בהן. במהלך הזמן הזה על מדינות להגדיר באופן מדוייק את הטכנולוגיות המדוברות; לדרוש הערכה שקופה של סיכונים לזכויות אדם בעסקאות מכירה כאלה; לקיים רישום ציבורי פתוח של כלים, חברות ולקוחות; ולקיים שימועים פתוחים בנוגע לעסקאות שהשלכותיהן רגישות במיוחד.

**סיכום ההמלצות של הדווח המיוחד נמצא בנספח ב.**

[19] Human Rights Council Forty-first session 24 June–12 July 2019 Agenda item 3 Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development; Surveillance and human rights Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; A/HRC/41/35; Recommendations 66.

וראו גם: Amir Cahane, "*Targeting targeted surveillance - The UN special rapporteur's report on the private surveillance industry*" CSRCL Blog (31.12.2021).

המכון הישראלי
לדמוקרטיה

**נקודה לדיון: פער רחב מידי בין ההסדר הישראלי ויישומו לבין הנורמות המקובלות בעולם המערבי, עלול להוביל לפגיעה ביכולת של תעשיית הסייבר המקומית להמשיך לייצא כראוי למדינות עולם ראשון.**

**נספח א: ההסדר האירופי החדש לפיקוח על יצוא מוצרים דו שימושיים**

התקנות האירופיות לפיקוח על ייצוא, תיווך, עזרה טכנית, שינוע והעברה של מוצרים דו שימושיים[20] (להלן: **תקנות יצוא מוצרים דו שימושיים**) פורסמו בחודש מאי 2021 ברשומות האיחוד האירופי, ויכנסו לתוקף בספטמבר 2021.

תקנות יצוא מוצרים דו שימושיים מחילות משטר של אישורים על ייצוא מוצרים דו שימושיים מהסוגים המנויים ברשימה שבתוספת הראשונה לתקנות,[21] ובנסיבות מסוימות גם על מוצרים שאינם מנויים בה.[22] משטר האישורים חל גם על תיווך בעסקאות רכש של מוצרים דו שימושיים, על שינועם, או על מתן תמיכה טכנית בנוגע אליהם[23] – אם נעשה בהם שימוש בקשר לפיתוח, הפעלה, תחזוקה, אחסנה, זיהוי או הפצה של נשק לא קונבנציונלי; שימוש לתכלית צבאית אם אחת מהמדינות המתקשרות נתונה תחת אמברגו; או אם נעשה בהם שימוש כרכיבים או חלקים במוצרים צבאיים המוגדרים ברשימות של מדינות חברות בתור שכאלה.[24]

אישורים יכולים להיות פרטניים (אישור שניתן ליצואן ספציפי לייצא מוצר דו שימושי ספציפי, אחד או יותר, למדינה ספציפית) או גלובליים (אישור שניתן ליצואן ספציפי ביחס לקטגוריה של פריטים דו שימושיים לייצא למדינה או מדינות יעד מוגדרות), ואז אלו יינתנו על ידי הרשות הלאומית המוסמכת, ויהיו תקפים למשך שנתיים.[25] כמו כן, תחת התקנות ניתן לייצא מוצרים דו שימושיים מסוימים בכפוף לעמידה בתנאי אישור אירופאים כלליים,[26] או בכפוף לעמידה בתנאי אישור לאומיים כלליים.[27]

כאשר הרשויות המוסמכות של מדינות חברות שוקלות אם לאשר או לדחות בקשות לאישורים גלובליים עליהן להביא בחשבון, בין השאר,[28] (1) התחייבויות בין לאומיות של האיחוד ושל מדינות חברות, ובפרט בקשר עם משטרי הפצת נשק בין לאומיים ואמנות בינלאומיות רלוונטיות; (2) התחייבויות תחת סנקציות שהוטלו על ידי מועצת אירופה או על ידי מועצת הביטחון של האומות המאוחדות; (3) היבטים של מדיניות חוץ וביטחון, לרבות העקרונות האירופיים לייצוא

---

[20] Regulation (EU) 2021/821, 2021 O.J. (L 206) 1, 1

[21] Regulation (EU) 2021/821, Art 3(1), 2021 O.J. (L 206) 1, 1

[22] ר' לדוגמא Regulation (EU) 2021/821, Art 4-5, 2021 O.J. (L 206) 1, 1

[23] Regulation (EU) 2021/821, Art 6-8, 2021 O.J. (L 206) 1, 1

[24] Regulation (EU) 2021/821, Art 4(1), 2021 O.J. (L 206) 1, 1

[25] Regulation (EU) 2021/821, Art 12, 2021 O.J. (L 206) 1, 1

[26] ר' חלקים A עד H לתוספת השנייה לתקנות יצוא מוצרים דו שימושיים.

[27] ר' ס' 12(6) לתקנות, וכן חלק C שבתוספת השלישית לתקנות יצוא מוצרים דו שימושיים.

[28] Regulation (EU) 2021/821, Art 15(1), 2021 O.J. (L 206) 1, 1

טכנולוגיה וציוד צבאיים,[29] ובתוכם העמדה לפיה לא יינתן רישיון ייצוא כאשר יש סיכון ברור שייעשה שימוש בטכנולוגיה או בציוד לדיכוי פנימי או להפרות הדין ההומניטרי הבינלאומי;[30] (4) שיקולים ביחס לשימוש הקצה שייעשה במוצר; וכן, (5) הטמעת תוכנית ציות פנימית (Internal Compliance Program) על ידי המייצא.[31]

התוספת הראשונה לתקנות מכילה רשימה של מוצרים דו שימושיים שייצואם חייב באישור,[32] ובתוכם ניתן למנות מערכות מחשב ייעודית לתוכנות חדירה (intrusion software),[33] תוכנות ייעודיות לחדירה,[34] טכנולוגיות לפיתוח של תוכנות חדירה,[35] וכן מערכות מעקב במרשתת (IP Network Communications Surveillance systems).[36]

התקנות אינן מגדירות מהי 'תוכנת חדירה', אך הן מגדירות מוצרי מעקב סייבר (Cyber Surveillance Items) כ'מוצרים דו שימושיים שעוצבו במיוחד על מנת לאפשר מעקב חשאי אחר אנשים באמצעות ניטור, חילוץ, איסוף או ניתוח נתונים ממערכות מידע ותקשורת אלקטרונית'.[37] התקנות מורות כי בנסיבות מסוימות, מוצרי מעקב סייבר כאמור יהיו חייבים באישור גם אם אינם מנויים בתוספת הראשונה.[38]

בכפוף להודעה של הרשות המוסמכת לפיה מוצרי מעקב סייבר (שאינם מנויים בתוספת הראשונה) ישמשו במדינת היעד לדיכוי פנימי, לפגיעה חמורה בזכויות אדם או להפרה חמורה של הדין ההומניטרי הבינלאומי, היצואן שלהם יהיה חייב באישור ייצוא.[39] אם בעקבות בדיקת נאותות נודע ליצואן כי מוצרי מעקב סייבר עשויים לשמש למטרות אלו

במדינת היעד, עליו ליידע את הרשות המוסמכת וזו תקבע אם נדרש אישור ייצוא.[40] תקנות יצוא מוצרים דו שימושיים מאפשרות למדינות החברות לקבוע בחקיקה לאומית דרישת אישור ייצוא במקרים בהם ליצואן ישנו חשד שמוצרי

---

[29] Common Position 2008/944/CFSP

[30] Common Position 2008/944/CFSP Art. 2(a)

[31] Regulation (EU) 2021/821, Art 15(2), 2021 O.J. (L 206) 1, 1

[32] Regulation (EU) 2021/821, Art 3(1), 2021 O.J. (L 206) 1, 1

[33] Regulation (EU) 2021/821, Annex I, Item 4A005, 2021 O.J. (L 206) 1, 1. התקנות אינן מגדירות מהי 'תוכנת חדירה'.

[34] Regulation (EU) 2021/821, Annex I, Item 4D005, 2021 O.J. (L 206) 1, 1

[35] Regulation (EU) 2021/821, Annex I, Item 4E001, 2021 O.J. (L 206) 1, 1

[36] Regulation (EU) 2021/821, Annex I, Item 5A001(j), 2021 O.J. (L 206) 1, 1

[37] Regulation (EU) 2021/821, Art. 2(20), 2021 O.J. (L 206) 1, 1

[38] משכך, חרף העמימות הפרשנית הנובע מהעדר הגדרה ל'תוכנות החדירה' המנויות בתוספת הראשונה, זיהוי מוצר דו שימושי כ'מוצר מעקב סייבר' עשוי להחיל עליו דרישה לאישור גם אם הוא לא תואם את הקטגוריות שבתוספת הראשונה.ר' Regulation (EU) 2021/821, Art. 5(1), 2021 O.J. (L 206) 1, 1

[39] Regulation (EU) 2021/821, Art. 5(1), 2021 O.J. (L 206) 1, 1

מעקב סייבר אלו עשויים לשמש למטרות אלו.[41] במסגרת הדיווחים השנתיים של הנציבות האירופית לפרלמנט האירופי ולמועצה האירופית על יישום התקנות, תהיה התייחסות מיוחדת לאישורי ייצוא של מוצרי מעקב סייבר.[42]

**נספח ב: המלצות הדווח המיוחד של האו"ם לגבי פיקוח על יצוא טכנולוגיות מעקב ואיסוף דו שימושיות, משנת 2019[43]**

For States:

(a) States should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place;

(b) States that purchase or use surveillance technologies ("purchasing States") should ensure that domestic laws permit their use only in accordance with the human rights standards of legality, necessity and legitimacy of objectives, and establish legal mechanisms of redress consistent with their obligation to provide victims of surveillance-related abuses with an effective remedy;

(c) Purchasing States should also establish mechanisms that ensure public or community approval, oversight and control of the purchase of surveillance technologies;

---

[40] Regulation (EU) 2021/821, Art. 5(2), 2021 O.J. (L 206) 1, 1

[41] Regulation (EU) 2021/821, Art. 5(3), 2021 O.J. (L 206) 1, 1

[42] Regulation (EU) 2021/821, Art. 26(2), 2021 O.J. (L 206) 1, 1

[43] Human Rights Council Forty-first session 24 June–12 July 2019 Agenda item 3 Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development; Surveillance and human rights Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; A/HRC/41/35; Recommendations 66.

(d) States that export or permit the export of surveillance technologies ("exporting States") should ensure that the relevant government agencies solicit public input and conduct multi-stakeholder consultations when they are processing applications for export licences. All records pertaining to export licences should be stored and made available to the greatest extent possible. They should also establish safe harbours for security research and exempt encryption items from export control restrictions;

(e) Exporting States should join the Wassenaar Arrangement and abide by its rules and standards to the extent that these are consistent with international human rights law;

(f) States participating in the Wassenaar Arrangement should develop a framework by which the licensing of any technology would be conditional upon a national human rights review and companies' compliance with the Guiding Principles on Business and Human Rights.

Such a framework could be developed through a specially established human rights working group. Additionally, they should set clear and enforceable guidelines on transparency and accountability with respect to licensing decisions, surveillance-related human rights abuses and the treatment of digital vulnerabilities.

For companies:

(a) Private surveillance companies should publicly affirm their responsibility to respect freedom of expression, privacy and related human rights, and integrate human rights due diligence processes from the earliest stages of product development and throughout their operations. These processes should establish human rights by design, regular consultations with civil society (particularly groups at risk of surveillance), and robust transparency reporting on business activities that have an impact on human rights;

(b) Companies should also put in place robust safeguards to ensure that any use of their products or services is compliant with human rights standards. These safeguards include contractual clauses that prohibit the customization, targeting, servicing or other use that violates international human rights law, technical design features to flag, prevent or mitigate misuse, and human rights audits and verification processes;

(c) When companies detect misuses of their products and services to commit human rights abuses, they should promptly report them to the relevant domestic, regional or international oversight bodies. They should also establish effective grievance and remedial mechanisms that enable victims of surveillance-related human rights abuses to submit complaints and seek redress. 68. For the United Nations: the Organization, particularly the Human Rights Council, should create a working group or cross-mandate task force to monitor and provide recommendations on trends in, and individual cases of, human rights abuses facilitated by digital surveillance.

For all stakeholders: States, the private sector, civil society and other relevant stakeholders should establish co-regulatory initiatives that develop rights-based standards of conduct for the private surveillance industry and implement these standards through independent audits, and learning and policy initiatives.