

שלום לכולם,

ביום רביעי שעבר (17.2.16) התקיים מפגש העוסקים בתחום הסייבר, בנושא טיטוט צו הפיקוח על יצוא מוצרי סייבר המציעה להרחיב את הפיקוח הקיים זה מכבר על ייצוא מוצרים, ידע ושירותים בתחום. מטרת הפגישה הייתה לאחד את התעשייה בנושא, להעלות הערות לטיטוט וכן לשמוע הצעות ודרכים לפעולה לשם שמירת האינטרסים של היזמים, סטארטאפסטים וחברות שונות בתעשייה. כמו כן ניתנה סקירה על הנעשה עד כה בנושא על ידי חברות ונותני שירותים שונים בתחום.

בפגישה לקחו חלק כ-36 חברות, יזמים ונציגים מסקטורים שונים בתחום וכן נציגים ממכון היצוא, ארגון לשכות המסחר והתאחדות התעשיינים. כמו כן, כיבד בנוכחותו נציג הרגולטור, ד"ר טל שטיינהרץ, CTO מטה הסייבר.

**זהו מפגש ראשון ותקדימי מסוגו שבו התאחדו ושיתפו פעולה מגוון רחב של עוסקים בתחום הכל בכדי ליצור חזית אחידה בהגנה על האינטרסים של התעשייה.** בין המשתתפים היו החברות: CyberRisk, Defensia, CheckPoint, Cymmetria, CheckMarx, ReSec, Athena, Mer Group, BioCatch, Secoz, Ernest EYoung, MetaPacket, ELbit CyberBit, Comsec, ABB, CyberSixGil, Israel Aerospace Industries, &Young, AI-LAW; משרדי עורכי הדין: HFN, GKH, AI-LAW, ליפא מאייר, גולדפרב זליגמן; ועוד יועצים מקצועיים לענייני אפ"י.

זו ההזדמנות להודות למובילים והמארגנים של המפגש: **Cyber Together** - בהובלתם של אלון רפאלי ואיסר זק ובשיתוף פעולה של עו"ד שחר אלון, **Checkmarx**; רפאל אבגי, **Defensia**; חברת **Cymmetria** בהובלתו של עו"ד יונתן ברוורמן; יורם גולדסקי ואייל הררי, **CyberRisk**; אריאל פלד, **DocAuthority**; ועו"ד אדמית אבגי, **AI-LAW**. כמו כן נבקש להודות לטל מוזס, **Ernest&Young** על האירוח.

בפגישה הוסבר, כי הטיטוט, מבקשת להרחיב את הרגולציה, הקיימת זה מכבר על התשתיות לתוכנות חדירה, לפיקוח על תוכנות החדירה עצמן, וכן מציעה להוסיף לפיקוח: כלי פורנזיקה בעלי רכיב פיזי, מוצרי הגנה המגינים על תשתיות אסטרטגיות, חולשות ומערכת או תוכנה שתוכננה או הותאמה במיוחד לאיתור חולשות אוטומאטי, לשם ביצוע שימוש בהם בתוכנת חדירה כנגד אחר.

כמו כן, הועברה סקירה על המשמעויות המשפטיות, העסקיות והכלכליות של הטיטוט וכן הוצגו מספר התייחסויות שגובשו זה מכבר על ידי חברות שונות. בנוסף, הוצגו הפעולות שנעשו עד כה בנושא. לאחר מכן הביעו את דעתם בנושא המשתתפים בפגישה והועלו הצעות לביצוע.

**להלן עיקרי הדברים שעלו בישיבה בראשי פרקים** (ראו הרחבה בנושאים השונים בתרשומת הפגישה המלאה בהמשך המסמך):

#### התייחסויות לטיטוט:

1. הרגולציה הקיימת זה מכבר בתחום הינה מספקת ועונה על האינטרסים שמבקש הרגולטור להגן עליהם בטיטוט המוצעת.
2. מדובר בטיטוט לצו השואב כוחו משני חוקים, בעלי סנקציה פלילית כדמות קנס ומאסר. בהקשר של יצוא בתחום הביטחוני, החוק אף מטיל אחריות אישית פלילית על נושא משרה בתאגיד. הרחבת הרגולציה ואי הבהירות שלה עלולה לסכן, הלכה למעשה כל עוסק בתחום לסנקציה פלילית.
3. טיטוט הצו חלה על כל אדם שעושה פעולת יצוא, בין אם מדובר באזרח, תושב, חברה ישראלית וחברה לא ישראלית וכד'.
4. ההגדרות המוצעות בטיטוט למוצרים, ידע ושירותים המבוקשים לפיקוח אינה ברורה ורחבה, דבר המכניס בגדרה אף חברות העוסקות בהגנת סייבר וכאלה שאין צורך שיהיו כלל מפוקחות.
5. כבר כיום ישנו נסיגה והיסוס מצד המשקיעים לאור הרגולציה
6. בהרחבת הרגולציה, מדינת ישראל מאבדת את היתרון התחרותי שלה בתחום הסייבר למול העולם.
7. הרחבת הרגולציה משיתה על, יזמים, חברות קטנות וסטארטאפים עלויות משמעותיות אשר אינן יכולות לעמוד בהן. דבר הפוגע באופן עקיף בחדשנות.
8. הליך ההיוועצות לכאורה של הרגולטור עם החברות הגדולות במשק, בטרם הוצאת הטיטוט, אינו תקין הואיל ולא כללה את כל הספקטרום - חברות עם גילאים שונים וסקטורים שונים.
9. לא מובן מה כוונת הרגולטור, מה אינטרסים שמבקש להגן עליהם מכאן אין ודאות ויכולת להשיג לגופו של עניין על הטיטוט.

10. הרגולטור מתבקש להסדיר את האתגרים שעומדים בפניו מבקש להתמודד בשיתוף מלא עם התעשייה.
11. הרגולטור מתבקש לדחות את מתן ההערות לטייטא בכדי לאפשר לתעשייה להתכונן בהתאם.
12. לבצע בחינה והסתגלות- לפרסם תחילה הנחיות בנושא ולבחון את היישום שלהן בשטח במשך שנה או שנתיים- מכאן לזהות מקרים ספציפיים בעייתיים ולסמן אותם.
13. הפיקוח אמור להיעשות על ידי משרד הכלכלה ולא משרד הביטחון.
14. ליצור הליך "פרה רולינג" אשר יאפשר לחברות באמצעותו לדעת האם צריכות להיות מפקחות או לא.
15. יש לבצע את הליך הרגולציה בהתאם להחלטות ממשלה קודמות בנושא ועמדת הממשלה על הפחתת רגולציה
16. להחריג יצוא למדינות מסוימות מהצו כגון ארה"ב ואירופה.

בסוף הפגישה הוחלט לאמץ את היוזמה של ארגון ה Cyber Together והובלתו, להקמתם של צוות טכנולוגי בהובלתו של רפאל אבגי וצוות משפטי בהובלתו של עוה"ד: אדמית אבגי, יונתן ברוורמן ושחר אלון, בשיתוף עם כלל הגורמים הרלוונטיים לליווי התהליך למול הרגולטור והועדות השונות.

כמו כן, נמסר כי בקרוב יפרסם Cyber Together מענה לטייטא. הנכם מוזמנים לשלוח הערות למייל [info@CyberTogether.org](mailto:info@CyberTogether.org) ולקחת חלק. כמו כן, Cyber Together קוראת לכל החברות לשלוח את ההערות שלהם לצו עד לתאריך שנקבע ושאלין במסמך זה כדי להחליף את העמדה של כל חברה וחברה.

באפשרותכם אף לשלוח הערות ולעשות שימוש במענה לטייטא שפרסמה חברת סימטריה בקבוצה בפייסבוק "הרחבת הפיקוח על יצוא מוצרי סייבר".

נעדכן בהמשך על התפתחויות בנושא.

בכל שאלה או הבהרה מוזמנים לפנות אלינו ישירות או בדף הפייסבוק של הקבוצה "הרחבת הפיקוח על יצוא מוצרי סייבר" <https://www.facebook.com/groups/1689800464600861>.

**\*תרשומת הפגישה הינה סיכום של העיקרים בה ואינה משקפת באופן מלא את הנאמר בה או את רוח הדברים שנאמרו.**

### תרשומת מפגש חברות סייבר 17.2.16

דברי פתיחה: איסר זק, CyberTogether; טל מוזס, Ernest & Young.

תחילת פגישה: סבב היכרות עם הנוכחים.

### תחילת דיון:

עו"ד אדמית אבגי, AI-LAW: סקירה משפטית על המשמעויות המשפטיות של הטייטא:

כיום במדינת ישראל, מוטל פיקוח על יצוא מוצרים, ידע ושירותים בתחום הסייבר מכוח פקודת היבוא והיצוא [נוסח חדש], התשל"ט – 1979, על פי צו היבוא והיצוא (פיקוח על יצוא טובין, שירותים וטכנולוגיה דו-שימושיים), תשס"ו-2006 ("צו היבוא והיצוא מוצרים דו-שימושיים"), בנוגע ליצוא ללקוחות אזוריים, בפיקוחו של משרד הכלכלה; וחוק הפיקוח על היצוא הביטחוני, תשס"ז – 2007, על פי צו הפיקוח על יצוא ביטחוני (ציוד דו-שימושי מפקח), התשס"ח – 2008 ("צו הפיקוח על היצוא הביטחוני מוצרים דו-שימושיים"), בנוגע ליצוא ללקוחות בטחוניים או מדינות, בפיקוח של משרד הביטחון- אפי".

הן צו הפיקוח על יצוא ביטחוני והן צו היבוא והיצוא, מוצרים דו-שימושיים, קובעים, כי המוצרים, ידע ושירותים אשר בפיקוח, מבוססים על הפריטים המנויים בהסדר ואסנר (Wassenaar)<sup>1</sup>.

החוקים והצווים לעיל מחילים על כל אדם (אזרח, תושב, חברה ישראלית ולא ישראלית) אשר מספק מוצרים, טכנולוגיה או שירותים ללקוחות זרים (פרטיים, ביטחוניים או מדינתיים) המנויים ברשימת ואסנר, ואשר עושים פעולת יצוא, חובה לפעול תחת רישיון יצוא ועוד. לצד זאת, קובעים החוקים והצווים עונשים פליליים החל מקנסות, עיצומים כספיים אזוריים ועד מאסר ממושך למפר. בהקשר של יצוא ביטחוני, נציין כי החוק

<sup>1</sup> הסדר ואסנר - הינו הסכם של מספר מדינות בדבר פיקוח על יצוא של אמצעי לחימה קונבנציונאליים פריטים וטכנולוגיות דו-שימושיים.

מטיל חובה אישית פלילית על נושא משרה בתאגיד (מנהל, דירקטור וכד') אשר יכל למנוע את ההפרה האמורה ולא עשה כן (יצוא ללא הרישיון).

בנוסף המוצע של הטיוטא, מבקשים להוסיף לרשימת הפריטים המנויים בהסדר ואסנר את הקטגוריות הבאות: פיקוח על תוכנות חדירה, חולשות, כלי פורנזיקס בעלי רכיב פיזי, מוצרי הגנה המגינים על תשתיות קריטיות ומערכת או תוכנה שתוכננה או הותאמה במיוחד לאיתור חולשות אוטומטיות לשם ביצוע שימוש בהן בתוכנת חדירה כנגד אחר, תוך הגדרה רחבה ועמומה של מושגים אלו.

נציין, כי בכל הקשור לתוכנת חדירה, בדיונים שנעשו בנושא על ידי מספר מדינות כדוגמת צרפת ובריטניה וכן מספר רב של גורמים כגון אגודות לזכויות אדם וכד', הוחלט לפקח אך ורק על הרכיבים בעייתיים בתוכנת החדירה המהווים תשתית ליכולות הבעייתיות בה, וכי אין כוונה לפקח על תוכנת החדירה כשלעצמה.

הוספה זו, בפועל, מרחיבה את הפיקוח על יצוא מוצרים, ידע ושירותים בעולם הסייבר אשר כיום לא מצויים בפיקוח, ואף הגדרתם הרחבה למעשה, חורגת ממטרות הפיקוח - דבר המהווה כבר כיום מכשול רב להתפחות התעשייה בארץ.

בנוסף, לאור מספרם הרב של הבקשות והביורוקרטיה הרבה שבתהליך הוצאת הרישיון, מתקשים הרגולטורים השונים, כבר כיום, לעמוד בזמני מתן הרישיונות הנדרש בחוק והרצון לקצור על ידי הרגולטור בלתי ישים. כמו כן, הדרישה שמוצר, ידע או שירות בתחום הסייבר יקבל רישיון כשלעצמו, הינו חסם משמעותי הפוגע בעסקאות עתידיות בתחום אשר מאופיינות בעיקרן בטווח זמנים קצר ביותר של שעות בודדות.

כעת יש להגיש הערות לטיוטא עד ה 3.3.16, ולאחריה תעבור הטיוטא הסופית לאישור ועדת החוץ והביטחון של הכנסת, ובמידה ותעבור ויהיו התנגדויות לה ניתן יהיה אולי להגיש בג"ץ.

הנכם מוזמנים להביע דעתכם על הנוסח המוצע מהאספקט האישי - מקצועי שאתם פועלים בו בכדי שנוכל לנסח מענה המגן על כמה שיותר אינטרסים של התעשייה.

**בקשה מהקהל:** אפשר לעשות סקירה למהם האינטרסים של הרגולטור?

**עו"ד אדמית אבגי:** אני מזמינה את ד"ר טל שטיינהרץ כנציג הרגולטור לענות על השאלה.

**ד"ר טל שטיינהרץ, CTO, מטה הסייבר:**

1. שמירה על שמה הטוב של המדינה: מדינת ישראל לא צריכה להפוך ליצואנית נשק סייבר במובן השלילי – הידע יכול להפוך לנשק.
2. יצוא נשק אמיתי שמגיע למקום הלא נכון – פוגע בזכויות אדם
3. אירוע יכול להחתים את כל התעשייה.
4. הבעיה בעולם של חולשות – הכי משמעותי להגנה

דחייה – מהות הערכה אם זה עניין של הערות

יש פער גדול בין המונח הטכנולוגי למונח המשפטי – למשל בחולשות

**עו"ד שחר אלון, יועמ"ש צ'ק מרקס, CyberTogether:**

צ'ק מרקס – עוסקת באיתור חולשות בקוד מקור (source code) בשלב הפיתוח, השוק העיקרי שלנו הוא בעיקר השוק האזרחי. הערותינו לטיוטא מתרכזות בכמה אספקטים:

1. מבחינת ההליך שהתבצע על ידי הרגולטור עד כה בעייתי. יש הרגשה שהייתה התייעצות עם חברות הגדולות בתעשייה בלבד והיא לא כללה את כל הספקטרום של התעשייה- חברות בגילאים שונים, היקפי פעילות, תחומי עיסוק וכו'. מכאן שלא התבצע הליך תקין ומסודר אל מול התעשייה למרות שטכנית אפ"י יכולים לטעון שכן ניתנה לחברות ההזדמנות להשמיע את טענותיהן. אם נגיע להתדינות משפטיות בעניין, הסיכוי שבית המשפט יתערב בשיקול הדעת המקצועי של הרגולטור הוא נמוך.

2. מצד הפרקטיקה- הדרישה של הרגולציה לחשוף את שמות הלקוחות הפוטנציאליים עומדת בסתירה להסכמי הסודיות (NDA) הנחתמים כבשגרה בעסקאות בתחום הסייבר. פיקוח של משרד הבטחון עלולה להעמיד את החברות הישראליות בנחיתות למול מתחרים אחרים מהעולם.

3. אנו מבקשים מהרגולטור לחשוף בפני התעשייה את האתגרים שהוא מנסה להתמודד עימם ולנסות להגיע לפתרון ביחד עם התעשייה ולא כ"הנחתה". הכוונה אולי מוצדקת אבל הדרך צריכה להיות שונה.

4. מוצע לבצע בחינה והסתגלות- לפרסם תחילה הנחיות ונהלים בנושא ולבחון את היישום שלהן בשטח במשך שנה או שנתיים.

5. אם יש בעיות או מקרים ספציפיים, יש לטפל בהם בצורה נקודתית. אפילו ראש אפי"י ציין שהצו החדש "לא יחול על 90% מחברות הסייבר הישראליות" – אז אנו שואלים, אם זה המצב? מדוע הוחלט להכניס לתזזית את כל התעשייה? עדיף שיזהו את אותן 10% מהחברות ולוודא שהתקנות יחולו רק עליהן. במצב הקיים לא ברור למי הטיוטא מכוונת.

6. קיימת חוסר ודאות בשאלה האם הרגולטור ימשיך עם הטיוטא בכל הכוח או שהוא הולך לשנות אותה, דבר היוצר חוסר ודאות בשוק.

7. ההמלצה שלנו – להשהות את התהליך, לבצע את העבודה המשותפת עם התעשייה ועם ארגונים כמו מכון הייצוא והתאחדות התעשיינים, ורק אז להתקדם.

### **נציג משרד עו"ד גולדפרב:**

מתבקש מהרגולטור להאריך את המועד – נמצאים בהליך התייעצות למול החברות בתחום – זו הדרך הנכונה בכל ענייני הרגולציה.

**אדמית:** נציין שהטיוטא הוצאה לתגובה בזמן שמתקיימים 3 הכנסים הגדולים והמשמעותיים ביותר בתחום הסייבר (סייבר טק 2016, קספרסקי ו-RSA) והחברות מרכזות את כל מאמצייהם וזמנם לכנסים אלו ומכאן שנדרשת הארכה.

### **נציג משרד עו"ד גולדפרב:**

לאחר מכן יעבור לדיון בכנסת למול ועדת החוץ והביטחון – מבקשים להקנות זכות טיעון לאנשים בתחום.

הניסוח הוא בעייתי – אני כיועמ"ש צריך להיות שמרן בכדי להימנע מאחריות פלילית.

לא ברור מי אמור לפקח – הפיקוח של משרד הכלכלה הוא מהיר. אם הרגולטור שהיה מפקח הוא משרד הכלכלה עם הזמנים המהירים בו הייתה קצת הרגעה. אולם בפועל זה יהיה תלוי, כל התחום הולך להיות צו אחד שיחליט שהרגולטור המפקח יהיה אפי"י. המקום צריך להיות במשרד הכלכלה ולא אפי"י.

**שטיינהרץ:** לא הוכרע מי הולך להיות הרגולטור.

**אדמית:** יש צוואר בקבוק בעניין שראש אפי"י צריך לאשר את הרישיון אז גם אם מיעלים את ההליכים הקיימים כיום זה לא ריאלי לעמוד בזמנים.

### **הערה מהקהל:**

לא מוטרד – אני יודע מה רוצים להשיג לא רוצים להקשות יש לראות איך ההליך זורם מהיר.

מה קורה עם ריסיילרים בחו"ל – הריסיילר לא יהיה מוכן שכל מגע יהיה מותנה אחורה יש לחשוב איך מונעים את זה.

עידן פוסט סנודן – מה המשמעות של פיקוח מראש – למה לא לשים חוק מול העיניים שיגדיר מה נכון או לא ולשים הליך פרה רולינג. העניין הכללי הוא גילוי היכולות – הסיכוי שאנחנו נחשוף משהו חדש לעולם הוא נמוך מאוד. אם נהיה ראשונים פוטנציאל ההכנסה הוא גדול.

איך ניתן לאכוף בכלל את הרגולציה?

### **עו"ד יונתן ברורמן, סימטריה:**

אני אתייחס לדברים מנקודת מבטו של מה יועץ משפטי פנימי של החברה מבין על זה. אציג את עמדת סימטריה כשם שפורסמה לכם – אומרים מה שכואב לנו וכל אחד יוסיף על הדברים. מוזמנים לעשות שימוש במסמך שהפצנו, להצטרף לה ולשלוח לנו הערות.

סימטריה עושה הכוונה תוקף deception. כואב לנו עניין הפורנזיקה – הצו לא חל עלינו אבל הצו הוא בנוי בצורה כל כך מרחיבה שיש להיכנס לקטגוריות שלו.

4 קטגוריות לפיקוח:

- פיקוח על תוכנות התקפיות
- חולשות – כולל איתור חולשות אוטומאטיים
- מוצרי סייבר הגנתיים – יועדו בהגנה במיוחד למערכות מסוימות. אם יש לי מערכת שניתן להתאים אותה ללקוחות שמפוקחים זה בעיה – יש לי בעיה להיכנס מבחינה כלכלית לתחום החדש.
- ציוד לחימה – כנראה שביטחוני ומפוקח – רכיב תקשורת ברמה הלאומית (מה זה?)

- מערכות של פורנזיקה דיגיטלית – לא קיימים בואסנר.

מתמקדים במערכות הפורנזיקיות:

מבחינה משפטית לא מבינים את הכוונה את התכלית. לא יכול לאזן את האינטרסים אם אני לא מבין את המטרה.

אין חובה בדין לצאת להתייעצות עם התעשייה – הייתה יוזמה שלהם שזה הליך טוב. אולם אם אני לא יודע מה הרגולטור רוצה אני לא יכול לאזן – אם אני לא יודע איך לאזן יש בעיה חוקית: חושב שזה מתאים לחוק ולא לצו.

אני יודע שפורנזיקה יש השפעה על עולם הביון.

הצו משקף פער טכנולוגי גדול בין מה שרוצים לפקח למה שהטכנולוגיה עושה. מהו ממשק פיזי (לשכפל הארד דיסק הוא ממשק פיזי? , דיסק און קי) אתה זה שלא מחליט בית המשפט הוא זה שיחליט והוא לא יודע להתמודד עם זה.

פקטור הזמן למתן הרישיון- 5 ימים זה יותר מדי – אם אני פוגש אדם ותוך 72 שעות אין את כל המידע ללקוח מאבד אותו. המתחרים הם מדינות אחרות שיכולות לספק את המוצר לפני ואז אני מאבד את הלקוח מאבד את החברה.

פער אודות האיומים- הפורנזיקה מנוסחת בצו כמי שנועדה לפגוע בביון. זה לא מה שאני רוצה – אני מפתח מביון עולמי ולא ישראלי – למה אני צריך להיות מוגבל כי אתם לא יכולים לפתח מערכת טובה יותר. הגבלה על מוצרי פורנזיקה יפגע ביכולת תההגנה של חברות בארץ אשר מאוימות מריגול עסקי של חברות מחו"ל.

הדרישה של הרישוי היא בעייתית היא מונעת לגשת ללקוח- הרישוי הוא בעייתי

פגיעה במיזמים- למה שהחברות הלא ישראליות הגדולות ישימו בארץ את מערכות הפיתוח שלהם בארץ?

פגיעה בחדשנות – אם מפתח מוצר עם כמה יכולות חוות דעת משפטית עולה כסף.

סטארטאפים וחברות קטנות נפגעות הכי הרבה – אין כוח אדם להתמודד עם הרישיון למול אפי".

הפאן המעשי – 2 נקודות- false negative, false positive – אם אני חושב שאני לא צריך לדווח וטעיתי אז המשמעות היא פליליות. תנו אמצעי לפרה רולינג – נציג קונספט – אם זה טעון פיקוח או לא ואם כן מי האדם הרלוונטי- לפי המפקח אוכל לדעת האם לפתח את המוצר או לא מבחינת כדאיות כלכלית.

אין סיכוי שתעמדו בלוחות הזמנים- מדובר בתעשייה השנייה הגדולה בעולם שוק מגלגל מיליארדים. אם לא עמדתם בזמן תנו לי את הרישיון אוטומאטי – אם לא רוצים לתת רישיון אוטומאטי תשפו על הנזק שנגרם לי כתוצאה מעיכוב מתן הרישיון. הרגולציה צריכה להיות דו-סיטרית.

שנדע מה הודאות שיהיה בעל בית שישפה ויפצה.

### נציג משרד עו"ד HFN:

להעביר הלאה כל התייחסות שאפשר לצו. כל דבר הוא חשוב.

### עו"ד הדר סטון משרד עו"ד GKH:

זווית חברות בינלאומיות- תסכול מהאי ודאות איך זה יושם מבחינת ה PT והפורנזיקה.

שאלה מהקהל: מה זה תוכנת תקיפה? – אם אין הגדרה מהי תקיפה הכל יכול להיכנס – קוצב לב, תוכנה רמזורים, דיאליזה.

רפאל אבני, דיפנסיה: DDOS מפוקח בנוסח? כן או לא?

שטיינהרץ: DDOS ככל הנראה לא נכנס לואסנר כי הוא לא מתחמק מגילוי

רפאל: חברת האמר למשל מספקת מוצר DDOS המתחמק מגילוי על ידי שינוי הפקטה באופן עצמאי כל פעם.

אם מטה הסייבר היה מולנו הוא היה מבין את הדינאמיקה במוצרי סייבר וכן היה מקבל הסברים מידיים על הבעייתיות שבפיקוח. למשל פיקוח על זירו דיי.

בנוגע להתייעצות שנעשתה עם החברות הגדולות - יש מספר שחקנים בשוק ולכל אחד האינטרס שלו – יש אינטרס לגדולים להישאר מפוקחים, יש להם יכולות ומשאבים וקשרים לכך למשל: חברות רב לאומיות – יש להם קשרים יכולים לקבל מבחינתם את הרגולציה. אם אני צריך לקנות סטארטאפ אני יכול להוריד לו את המחיר בגלל שהוא צריך להיות מפוקח ואני יודע שאין לו את המשאבים.

חברות ישראליות קטנות- יש להם בעיה איך להתמודד עם התקנות החדשות ולהבין לאן הולכים לשם. סלברייט למשל עלולה להיפגע אבל משיקוליה שלה לא רוצים להיות שותפים (טומנים את הראש בחול) יש כאלה שאומרים שאחרים יעשו את העבודה. אולם יש להתאחד ולעשות שיח עם כולם בכדי להמשיך ולהצמיח את התעשייה. הפיקוח אמור להיעשות בעדינות. הפורום הוא דוגמא לאוסף הבעיות שהתקנות מצמיחות.

אני אומר כן אבל – לבחון את הדברים בצורה שיטתית.

הגורמים המפקחים ידעו על מה הם מפקחים והגורמים המפקוחים ידעו על מה הפיקוח.

רוצים דו-שיח שנגיע לעמק השווה

**אביב חצבני, נציג התאחדות התעשיינים:** הממשלה קבעה הליך לרגולציה חדשה ובסוף הדרך לנתח מה המשמעות מבחינה כלכלית של הרגולטור מצד אחד לתעשייה ומצד שני- אם הממשלה הביאה מנגנון רלוונטי איך בוחנים את הרגולציה בשיתוף עם התעשייה – יש להשתמש במנגנון הזה.

התהליך הוא יעיל ועובד טוב.

ישנה החלטת ממשלה שדנה בהערכת רגולציה חדשה- כל רגולציה צריכה לעבור בתחילת שנה קלנדרית 1.1 – להחיל את זה על התקנה הספציפית

**אחיאז אלטר, מנהל תחום הסייבר, מכון היצוא:** הפתיחות של הרגולטור היא מבורכת. אני חושב שזו לא הייתה כוונת המשורר בניסוחים. רוב הנקודות עלו בשאר המקומות – אני חושב שיש לרכז מסמך או כמה עם כל הדברים. המטרה היא לא להגביל את היצוא – לקדם את התעשייה (בונים יחידת סייבר במכון היצוא) היא שונה ממה שמפוקח באפ"י. יש להעביר את הכל. חשוב להגיד למה לא – חשוב להגיד למה כן. לתת הצעות אופרטיביות לעניין הניסוח.

**רפאל:** אם הידע קיים בחו"ל ואני מוכר אותה בישראל – מה איכפת למדינה שאני עושה את זה. מדובר בחולשה שיש בעולם.

**אחיאז:** שהתעשייה תביא הצעות לניסוח

**איסר, CyberTogether:** הגדרה מבחינה מקצועית מתוך התעשייה – איך אנשי המקצוע צריכים להגדיר. מדובר במשהו שנקבע או משתנה.

אפ"י זה לא הגוף הנכון לפיקוח

**טל מוזס:** איך החברות בחו"ל תופסות את זה – הגיע חברה שמתעסקת בביטוחי סייבר לראות איזה חברה הם יכולים לעשות שימוש בשירותיה. אולם נושא הפיקוח היווה חלק מהשיקולים שלה.

**איסר:** יש ערוץ מקצועי שיש לנהל אותו מבחינה מסודרת עם כלל התעשייה- צריך נציגים ודו-שיח משפטי.

**ניר קרובבסקי, מטה פקט:** מציע להחריג את ארה"ב ואיחוד האירופי כך לא יכלל בצו.

**הערה מהקהל, נציג לשעבר ממשד הכלכלה:** יש עדכון של ואסנר 2015 – שמכסה את הנושא

רוב החברות עושות כבר את התהליך של פרה רולינג

דו-שימושי – כל מה שמתייחס להתאמה לכלי צבאי שמופיע בדו-שימושי הוא מפוקח – גם הפרשנות המרחיבה היום אפשר לעשות לרוב הדברים.

אני חושב שה-10% כבר מכוסים ברגולציה הקיימת – אם יש משהו לא מכוסה אפשר לפנות באופן ספציפי.

ניתן לעשות את הסחר בתיווך ולא להביא אותו לארץ.

הקרקע היום קיימת יש לתת לה פרשנות.

חברות קטנות לא מבינות את ההשלכות ואם לא מסייעים להם הם לא ידעו.

אם מוצר אזרחי יהיה בפיקוח הדבר הראשון שאומרים שלא מוכרים את זה. היצוא הישראלי נפגע בלא מאט פעילות בגלל הפרשנות המרחיבה- הפרשנות צריכה להיות מאוד מדויקת כמו שהיא מוגדרת בואסנר.

עדכון- רשימות החימוש בעברית ולא מתעדכנות לעומת ואסנר שמתעדכן משנה לשנה. יכול להיות שיש עדכון והוציאו מוצר אולם בארץ זה לא מעודכן.

אני מכיר את כל השיקולים של החוק – עצם העובדה שאנחנו אוטומאטית מוכלים בדו-שימושי יש פגיעה משמעותית. צריכים להיות מאוד זהירים.

**רון מוריץ, יו"ר CyberTogether:** מדבר מפרספקטיבה של משקיע - לא חושב שיש מקום בארץ לרגולציה כזו- אנחנו נחשבים כסוג של שוויץ מבחינה רגולטורית.

ארה"ב כן מכותבת עם ואסנר לא חתמו על החידוש על הסייבר- בארה"ב זה מתגלגל בקונגרס זה לא התקדם כי תעשיית הסייבר עמדה כנגד זה – אמרו שאנחנו עם חוק כזה לא יכולים להתחרות עם מדינות שאין להם חוק כזה- הצביעו על ישראל שהיא מדינה מובילה בגלל שאין לה רגולציה כזו.

אנחנו מקבלים כסף והשקעות מכל פינה שבעולם כולל מדינות ערביות, סין רוסיה ומצד שני יש את היכולת למכור לכל מדינה בעולם באופן חופשי זה מה שנותן לנו את היתרון התחרותי.

אני חושב שלא צריך לעשות רגולציה ולהמשיך לתת את התעשייה לזרום כמו עכשיו.

יסגור את הברז של המשקיעים את היכולת למכור למדינות – המקום שלנו של יצואן סייבר שני בעולם ייפול

**מלווה תעשיות באפ"י:** יש ניסיון של אפ"י לנסות להקל על סעיף 21 מוצרי הום לנד- ניסו להקל, אולם הישיבה התפוצצה. המצב של אפ"י למול ועדת חוץ וביטחון הוא לא טוב. אתגר להגיע מוקדם ולנסות לעשות מהר יותר ממה שהתכוונתם – מוכן לסייע עם מערכות ההיכרות.

יש באפ"י הליך של פרה רולינג התהליך שלה איטי- יש לעשות ועדה משותפת תחולה סייברית שתשחרר את הלחצים. שתהיה ועדה בשיתוף עם גופים רלוונטים באפ"י.

**גולדפרב:** הערה פרקטית- לייצר שולחן דיונים בצד המשפטי וקונספטואלי

נשמח לעשות שולחן עגול למה שצריך.

**אלון רפאלי, CyberTogether:** אנחנו יוזמים הקמה של צוות משפטי וטכני שייצגו את התעשייה בנושא וילוו את התהליך למול הרגולטור והוועדות השונות בו. נעדכן בנושא בהקדם. כמו כן בקרוב נפרסם את המענה שלנו לטיוטא המוצעת שתיקח בחשבון את כל האספקים שנאמרו פה.

תודה לכולם, - סוף דיון -