כלכליסט

מזרח תיכון חדש או איום ביטחוני במלכודת דבש

מה עושים בכירי צה"ל, השב"כ והמוסד לשעבר שרוצים למכור שירותי סייבר למדינה ערבית שאין לישראל יחסים דיפלומטיים עמה? ומה יעשו אם אותה מדינה תבקש שימכרו לה גם שירותי סייבר אסורים?; כך הסתבכו שלוש חברות בבעלות ישראלים באבטחת פרויקט תשתיות במפרץ הפרסי

תומר גנון והגר רבט 19.09.20 14:20

הסכמי השלום שנחתמו שלשום בין ישראל לאיחוד האמירויות ובחריין מבטיחים לנו יעד אקזוטי חדש לתיירות ועסקים. אלא ששעות ספורות לאחר ההכרזה בחודש שעבר על "הסכם אברהם", כפי שכונה ההסכם עם איחוד האמירויות, החלו להתפרסם עדויות של בעלים ועובדים בחברות טכנולוגיה וסייבר ישראליות שכבר חתמו על חוזי עבודה במדינה המוסלמית לפני שנים רבות, בחשאיות.

קראו עוד בכלכליסט:

- לא מבזבזים זמן: משקיעים ישראלים כבר נוהרים לנדל"ן באמירויות
- שר המסחר של דובאי: "בהסכם השלום יש פוטנציאל סחר של מיליארד דולר בשנה"
- ישראל חתמה על הסכמי שלום עם איחוד האמירויות ובחריין

כל עוד העסקאות הללו נחתמו מול מדינות עם אופי סובלני ומתון יחסית לישראלים, כמו איחוד האמירויות, אפשר היה לישון בשקט, אבל זה לא תמיד המצב. בכירים לשעבר במערכת הביטחון מעידים כי ממשלת ישראל ומערכת הביטחון

ספק ידעו ספק התעלמו מכך שבמשך שנים רבות חברות ישראליות עשו עסקים במדינות מפרץ נוספות שלישראל אין איתן יחסים דיפלומטיים, וגם כנראה לא יהיו לאור בריתות שונות עם מדינות אויב כמו איראן או קרבה רעיונית אליה בשאלת הסכסוך הישראלי־פלסטיני.

מימין: דרור מור, יואב פולי מרדכי ופיני מידן שני צילומים: יאיר שגיא, עמית שעל

סכסוך משפטי שפרץ בחודש יולי האחרון בין שלוש חברות, וחלק מפרטיו מתפרסמים כאן לראשונה, חושף מעורבות של ישראלים — כולם בכירי מערכת הביטחון לשעבר — באבטחה פיזית ואבטחת סייבר של פרויקט תשתיות אזרחיות גדול במדינת מפרץ פרסי שלישראל אין כיום יחסים דיפלומטיים איתה. על פרטי הפרשה הוטל תחילה צו איסור פרסום גורף על ידי בית המשפט המחוזי בתל אביב, לבקשת החברות המעורבות. בעקבות עתירת "כלכליסט",

באמצעות עו"ד ירון חנין ממשרד ליבליך מוזר, צמצמה לאחרונה השופטת חנה פלינר את הצו כך שהוא חל בעיקר על שם המדינה והפרויקט עצמו.

המסמכים שהותרו לפרסום חושפים טענות חמורות על ניסיון להוציא לכאורה מישראל ידע לביצוע תקיפות סייבר ללא רישיון ממשרד הביטחון. אף שהטענות האלה הוכחשו בהמשך על ידי הצדדים לסכסוך, לאחר עתירת "כלכליסט" לצמצום איסור הפרסום ופשרה כספית שנחתמה בין הצדדים, הן ממחישות את הסכנה הטמונה ב"גן העדן העסקי" במפרץ הפרסי, שעלול לשמש כמלכודת דבש להוצאת ידע ביטחוני רגיש מישראל.

הקשר בין מקורבו של ברק למקורבו של שרון

הסיפור החל לפי כשנתיים, כששלוש חברות שהקימו בכירים לשעבר בצה"ל, המוסד והשב"כ חתמו על חוזים בהיקף של מיליוני יורו לשמש כצוות הבדיקה והביקורת ("red team") של פרויקט תשתיות אזרחיות גדול באותה מדינת מפרץ.

החברה הראשונה היא שדמה (Sdema), חברה שהקימו בכירי השב"כ לשעבר דרור מור, שלמה הר נוי ודן וסלי, שהיו קשורים גם לראשי הממשלה השונים: הר נוי מונה לאחר רצח רבין למפקד היחידה לאבטחת אישים, ואילו מור היה מנהל אגף בשב"כ. כמו כן הוא חברו הקרוב של עמרי שרון, בנו של אריאל שרון, ושימש כעד אופי בשלב הטיעונים במשפט נגדו ב־2006. וסלי, ששירת בשב"כ שלושה עשורים, היה בתפקידו האחרון ראש אגף משאבי אנוש של הארגון. הר נוי מסר כי מכר את מניותיו בשדמה במרץ 2019 (בטרם ההסכם של החברה עם מדינת המפרץ שלישראל אין יחסים דיפלומטיים איתה).

שדמה פועלת הן בייעוץ בתחום האבטחה הפיזית (בדיקת המיגון של מתקנים ומבנים מאיומי טרור פיזיים כגון מכונית תופת, ירי, חדירת מחבלים וכו'), והן בסייבר הגנתי — כלומר חשיפת פרצות בשרתים ומחשבים כדי לסכל תקיפת סייבר, שתביא להשבתת מערכות או גניבת מידע. שדמה גויסה כספקית השירותים למדינת המפרץ. אלא שלאותה מדינה, כאמור, אין יחסים דיפלומטיים עם ישראל. כאן נכנסת לתמונה החברה השנייה בסיפור — נובארד (Novard).

נובארד הוקמה לפני כשנתיים בידי אלוף (מיל') יואב (פולי) מרדכי, לשעבר דובר צה"ל, מתאם פעולות הממשלה בשטחים וראש המינהל האזרחי, ובידי שון בוטר, עד לאחרונה בכיר במוסד. השניים מחזיקים כל אחד ב־25% מהחברה, וב־50% הנותרים מחזיקה חברה שבשליטת גיל גבע, יו"ר ומייסד חברת הנדל"ן תדהר, שמשמש כשותף לא פעיל. מרדכי ובוטר החליטו למנף את הקשרים והניסיון שצברו במערכת הביטחון כדי לספק שירותי ייעוץ ופיתוח

עסקי שיהוו "גשר בין עולם העסקים הגלובלי למזרח התיכון", כלשון אתר החברה. בסיפור הנוכחי שימשה נובארד המתווכת, זו שחיברה בין שדמה, הקבלן, למדינת המפרץ, הלקוח, בפרויקט התשתיות האזרחיות.

אולם בהיעדר יחסים דיפלומטיים, שיתוף פעולה בין חברה ישראלית למדינת המפרץ אינו מותר, ולכן נדרשה לעסקה חברה שלישית שתשמש ה"פרונט" שלה, כלומר חברת זרה שתהיה חתומה על העבודה ששדמה תספק בפועל.
לתפקיד הזה גויסה לגאסי טכנולוגיות (Legacy), חברה גרמנית ששניים מבעליה הם ישראלים: גיל בירגר ופיני מידן־שני. בירגר שימש בעבר כנספח כלכלי בשגרירות ישראל בוושינגטון, ונמנה עם צוות המייסדים של חברת הלובי RSLB, לצד יובל רבין, מנכ"ל משרד ראש הממשלה לשעבר שמעון שבס והרמטכ"ל המנוח אמנון ליפקין שחק. ואילו מידן הוא איש מוסד לשעבר ששימש כיועצו המדיני של אהוד ברק כשהיה ראש ממשלה.

בראיון ל"כלכליסט" בחודש שעבר, לאחר שפורסם על הסכם השלום הקרוב עם האמירויות, סיפר מידן שהוא פעיל במדינות המפרץ הפרסי כבר מ־2012, ולדבריו אחד הפרויקטים הראשונים שלו שם היה פרויקט חקלאי יחד עם ליפקין שחק. כיום הוא "מייצג חברות סייבר שונות" באזור, כמו גם את "התעשיות הישראליות הביטחוניות הגדולות שאותן הוא מייצג עם שותפים". כשנשאל על הצורך באישור אגף הפיקוח על היצוא הביטחוני (אפ"י) לגבי פעילות סייבר באמירויות, אמר מידן: "במשך תקופה ארוכה החברות הישראליות הגיעו להסכמות שאפשרו את שיתוף הפעולה הזה. ולאור זהות האינטרסים, תאימות האיומים המשותפים והאינטרס הכלכלי המשותף — החלה להתקיים פעילות אינטנסיבית מאוד".

לגאסי היא חברת סייבר בעצמה, שמפעילה מערכת ששמה NEO ומתוארת באתר החברה כ"מזהה פרצות בתשתיות IT בצורה אוטומטית ובזמן אמת, ומציעה הגנה אקטיבית נגד סיכונים הנגרמים מטעות אנוש". עם זאת, תפקידה בפרויקט, לטענת שדמה, היה כיסוי בלבד. "לגאסי פעלה בחסותה ובשליחותה של נובארד, בין היתר על מנת להסתיר את זהותה הישראלית", נטען בתביעה.
"שלב המו"מ (לחוזה מול מדינת המפרץ — ת"ג וה"ר) שבו הייתי מעורב באופן אישי", נכתב בתצהיר שהגיש לבית המשפט מור, מנכ"ל שדמה, ומתאר את רקיחת העסקה.

"התנהל במלואו בין קבוצת נובארד לבין שדמה. אלא שנוכח מצב היחסים בין ישראל לבין מדינת המפרץ והרגישות המתבקשת מכך, כמו גם סירובה של שדמה לקבל לידיה כספים מעבר לתמורה עבור ביצוע הפרויקט (צדדים שלישיים

איך עובדים עם מדינה שאסור לעבוד איתה

שאינם ידועים לה), הוחלט על ידי נובארד כי ההתקשרות תתבצע באמצעות לגאסי, חברה המאוגדת בגרמניה, שפעלה בשמה ובשליחותה של נובארד. הלכה למעשה מטרתה היתה להוות צינור להעברת כספים בלבד". התביעה של שדמה, בסכום שנאסר בפרסום, היתה נגד החלפתה בפרויקט, לטענתה לאור התנגדותה לספק למדינת המפרץ את מה שאסור, והיא הסתיימה כאמור בפשרה כספית בסכום לא ידוע.

מי רוצה למכור סודות ביטחוניים?

בחזרה לסכסוך. שני הסכמים שונים נחתמו סביב פרויקט התשתיות האזרחיות במדינת המפרץ הפרסי. הראשון באוקטובר 2018, בשלב ההיערכות הביטחונית של הפרויקט האזרחי, בין מדינת המפרץ ללגאסי, והשני נחתם באוגוסט 2019 בין שדמה ללגאסי. על פי התביעה, "שדמה נענתה להצעה לאחר שהתקבלו האישורים הנדרשים מהאגף לפיקוח על היצוא הביטחוני במשרד הביטחון (אפ"י)".

שדמה, כך נטען, החלה בהיערכות לביצוע בפועל של השירותים לבחינת האבטחה הפיזית ואבטחת הסייבר בפרויקט, אלא שאז נדלקה אצלה נורה אדומה והיא טענה שסולקה מהפרויקט, ובשל כך היא הגישה תביעה לבית המשפט וצירפה לה את תצהירו של מור. "התעורר אצלנו חשש כי בניגוד לשירותים הנדרשים משדמה על פי ההסכם, מדינת

המפרץ אינה מבקשת לקבל רק פתרונות להגנה מפני מתקפות סייבר (סייבר הגנתי) אלא גם ידע ויכולות סייבר התקפיים", כתב מור בתצהירו.

סייבר התקפי הוא סיפור אחר לגמרי מכלי הגנת סייבר, ומקיף רשת רחבה של יכולות ופעולות, מווירוסים ומתקפות שיכולות לגרום לנזק בל יתואר ועד כלי רוגלה ומעקב המשמשים לאיסוף מידע אזרחי או ביטחוני. אמנות בינלאומיות שונות קובעות שכלי תקיפה ומעקב כאלה נחשבים לכלי נשק וצריכים לעמוד בהגבלות יצוא דומות. מור לא פירט כמובן אילו ידע ויכולות התקפיים מצויים ברשות שדמה, אך בתצהיר שלו התריע כי "שדמה מודעת למידת הנזק שידע ביטחוני בתחום הסייבר ההתקפי יכול לעשות, ולאיסור על העברת ידע מסוג זה ללא רישיון", ועל כן "סירבה לדון ובטח ובטח שלא להעבירו".

איזו פעילות כן כלל החוזה? לפי התצהיר של מור, "שדמה התחייבה במסגרת ההסכם לסייע למדינת המפרץ באיתור פרצות ופגיעות בתחום אבטחת הסייבר וטיפול בהן באמצעות בדיקות חדירות (Penetration Tests — PT), יכולת המהווה בפועל את ליבת הפרויקט (חשיפת פרצות אבטחה — ת"ג וה"ר). כן התחייבה שדמה לסייע בהכשרות בסיסיות לצוותי מדינת המפרץ, באמצעות מסירת ישויות (כ־100 לפחות על פי התביעה — ת"ג וה"ר) לביצוע בדיקות חדירות על ידי מדינת המפרץ... אין קשר בין שירותים אלו לבין דרישות מדינת המפרץ בתחום הסייבר ההתקפי".

בדצמבר 2019 נפגשו הצדדים ושדמה הציעה לנציגי מדינת המפרץ הפרסי "פתרונות חלופיים העולים בקנה אחד עם הוראות הדין וכללי הזהירות המתחייבים". אבל זה לא עזר. "למרבה הפליאה", כותב מור, "במרץ 2020, מסיבות שאינן מובנות לשדמה, 'התהפכה' לפתע מדינת המפרץ ועמה נובארד ולגאסי. אלו דרשו כי שדמה תעביר למדינת המפרץ לאלתר מסמך כתוב אשר יכיל את הידע וטכנולוגיות הסייבר ההתקפיות הרגישות. משסירבה שדמה, הודיעה לגאסי לשדמה על ביטול ההסכם". לדברי מור, נובארד ולגאסי התרעמו על הסירוב של שדמה ו"טענו כי היא מעוררת מהומה רבה על לא דבר". נובארד ולגאסי מכחישות בתוקף את הטענות (ראו תגובתן בסוף הכתבה) הללו.

זמן קצר לאחר הגשת התביעה שלוש החברות הודיעו לבית המשפט כי פנו לבוררות והגיעו להסכם ביניהן שכולל פיצוי כספי לשדמה. לאחר הפשרה נסוגה שדמה מטענותיה, ונציג החברה דן וסלי אמר בדיון שנערך בבית המשפט בבקשת "כלכליסט" להסרת צו איסור הפרסום כי "הטענה כיום בדבר סייבר התקפי לא רלבנטית ולא קיימת לאחר שראיתי את המסמכים והעובדות שהוצגו לי".

אחד מתלונן מטעם החברה, שני מתחרט בשמה

מה גרם לשדמה לחשוד בטוהר הכוונות של מדינת המפרץ? לפי כתב התביעה, דברים שנאמרו ומסמכים שהתבקשו מנציגי מדינת המפרץ במסגרת פגישות מקדימות שנערכו בין הצדדים באירופה. "בשבוע השני של נובמבר 2019", נטען בתצהיר של מנכ"ל שדמה, "נערכה סדנת עבודה ראשונה בתחום הסייבר בלונדון, בנוכחות נציגי מדינת המפרץ, שדמה ונובארד (...), נציגי מדינת המפרץ ביקשו, בניגוד להוראות ההסכם, מסמך המפרט את התשתיות שיאפשרו לה להתחיל לבנות את הרשתות הנדרשות".

סייבר מתחת לשולחן

לפי התצהיר של מנכ"ל שדמה, ב־24 בנובמבר שלח אפי ירושלמי, מנהל הפרויקט מטעם נובארד, מייל למנכ"ל שדמה שבו כתב כי בעקבות פערים בהבנת נציגי מדינת המפרץ את תוצרי הפרויקט שאותם היא אמורה לקבל בהתאם להסכם, יש צורך "ליישר קו" בין נובארד לשדמה. "על מנת שלא לגרום סכסוך מיותר, באותו יום שלחתי הודעה שבה התייחסתי לפעולות שבכוונת שדמה לנקוט, ובהן בין היתר העברה מיידית של מסמך החומרה שעל מדינת המפרץ לרכוש ולהקים לצורך ביצוע בדיקות חדירות (חשיפת פרצות — ת"ג וה"ר) באופן עצמאי", נכתב בתצהיר של מור, אולם "למדינת המפרץ היו תוכניות אחרות (כך התברר לשדמה בדיעבד)".

ב־1 בדצמבר 2019 שלח נציג מדינת המפרץ מייל ללגאסי, חברת הצינור, שבו, נטען בתצהיר, "דרש לראשונה נציג מדינת המפרץ לקבל בתוך כ־4 ימים בלבד מסמך אשר יכונה 'מסמך הסייבר ההתקפי'. דרישה זו הפתיעה את שדמה, שכן הרכיבים שפורטו הם מתחום הסייבר ההתקפי, תחום אשר כלל לא נזכר בהסכם שהוכן על ידי הצדדים לאחר

פגישתם בלונדון, וממילא שדמה מעולם לא הסכימה לדון בשיווק סייבר התקפי ובטח ובטח לא להעבירו לידי מדינת המפרץ.

"בעקבות הודעת הדוא"ל של נציג מדינת המפרץ החל לקנן בלבה של שדמה חשש כי אותה מדינה לא מעוניינת רק בהכשרה מקצועית לשיפור עצמאי של מערכי ההגנה, אלא גם בקבלה של ידע ישראלי מן המוכן לביצוע תקיפות סייבר (...) המשמעות האופרטיבית היא העברת ידע התקפי לידיו של גורם זר".

האם באמת היה ניסיון להוציא ידע סייבר התקפי מישראל באמצעות חוזה אזרחי? מהמסמכים שהותרו לפרסום לא ניתן לקבוע. מצד אחד, ישנו תצהיר לבית המשפט, מסמך מחייב משפטית שבו מתחייב מנכ"ל שדמה לומר את האמת. בתצהיר הזה מור טוען כי נעשה ניסיון להוציא מחברתו ידע סייבר התקפי. מצד שני, שדמה חזרה בה מטענתה, אבל זה נעשה רק לאחר העתירה להסרת איסור הפרסום והפשרה הכספית בין שדמה לנובארד ובאמצעות גורם אחר בחברה — כלומר במקום מור, שחתום על התצהיר המחייב, פנה וסלי לבית המשפט ומסר כי בדיעבד, לאחר שקיבל הסברים והציגו לו מסמכים, הטענה כבר לא רלבנטית.

מנובארד נמסר בתגובה: "נובארד פועלת בתחומי טכנולוגיה, תשתיות אזרחיות והשקעות בלבד. החברה לא פעלה ואינה פועלת בתחומי הסייבר ההתקפי. מדובר בציטוטים מתוך טענות שהעלתה חברת שדמה במסגרת חילוקי דעות מסחריים גרידא, ואשר מהן היא חזרה לאחר זמן קצר, לרבות בהצהרה מפורשת בפני בית המשפט. כיום לא מתנהלים כל הליכים משפטיים בין הצדדים".
מלגאסי נמסר: "לגאסי הנה חברה זרה הפועלת על פי חוק, ומנהליה מכחישים את כל הטענות שהועלו בכתבה".