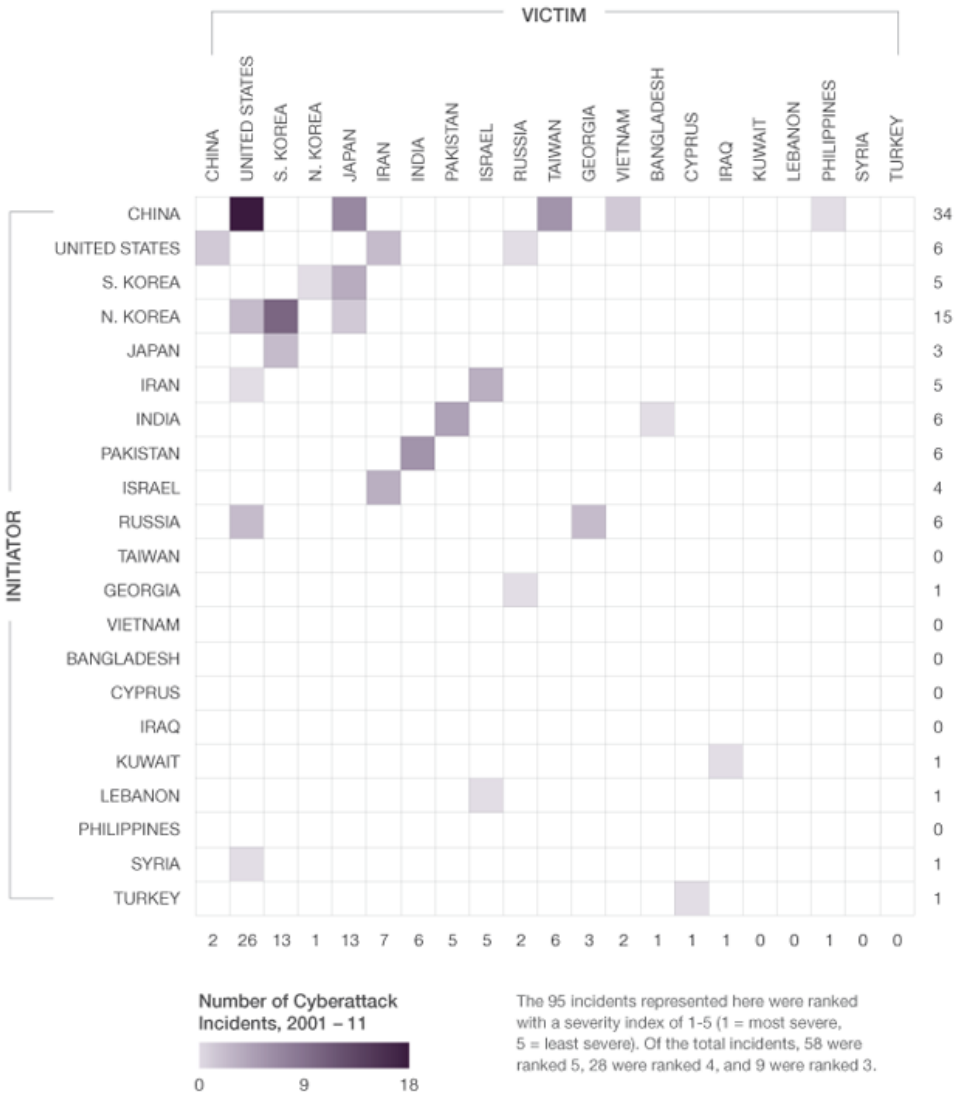
'האימפריה מכה שנית' – סוגיות עכשוויות בהתארגנות המדינתית לסייבר באמריקה

רשמים מתוך מפגשים בוושינגטון, אוקטובר 2012

ד"ר עפרה גרייצר

בכל יום מתבצעות למעלה מ-100 מתקפות סייבר על סוכנויות ממשלתיות...



תוכן עניינים

כיצד משנה הסייבר את שיח הבטחון הלאומי?

(1) האם סייבר מחדש אסטרטגית?

(2) הקבלה בין המימד הקינטי למימד הקיברנטי

(3) עיצוב כללי המשחק האסטרטגיים (סייבר והחוק הבינלאומי)

מהו אפקט סייבר?

(4) שיחים אנלוגיים לסייבר - גרעין ולוחמה לא-סדירה

(5) מהו איום הייחוס? ייחשב 'פרל הרבור' בסייבר?

(6) פרדוכס מידת הקידמה כמידת הפגיעות

(7) מיהו היריב?

(8) הפללה (attribution) ו/או היכולת לממש 'הרתעה' בסייבר

(9) דיפלומטיית סייבר - מחלקת המדינה

(10) מיליטריזציה של מרחב הסייבר

כיצד מתארגנים להגנה מדינתית בסייבר?

גניאלוגיה של מרחב הסייבר - התהוות מתוך ישויות ארגוניות/ פיקודיות קיימות

מתחים בחלוקת הסמכות, האחריות וסדר-העדיפויות המדינתיים

נקודות-המבט המעצבות מדיניות והסדרה של השוק האזרחי בהיבט ההגנתי:

הגנת המדינה - מקומו של פיקוד הסייבר במערכת

תשתיות קריטיות

ניטור האינטרנט ואבטחת-מידע

רגולציה ומשמעויותיה

מגמות תרחישיות בהתפתחות של מרחב הסייבר והגנתו

מה ניתן להקיש מהמקרה האמריקאי להקשר הישראלי?

כיצד משנה הסייבר את שיח הבטחון הלאומי?

שיח הסייבר באמריקה רווי בחוסר-הסכמות, הנובעות משני מושכים מנוגדים על פניהם: מחד, זהו מרחב חדש מעשה ידי-אדם, הדורש סידור מחדש של דפוסים קיימים או יצירה של דפוסים חדשים (מהפכני); מאידך, מרחב הסייבר משקף את המציאות הקיימת על מתחיה התרבותיים, פוליטיים, חברתיים, פיקודים וארגוניים. במובן זה, יש כאן רצף או המשכיות של הקיים - פשיעה, עימותים בין מדינות, מאבק על זכויות הפרט וחופש הביטוי...(אבולוציוני). לכן, העיסוק אינו צריך להיות בביטחון-סייבר גרידא, אלא כחלק מהעיסוק בסוגיות של ביטחון לאומי:

(1) <u>האם סייבר מחדש אסטרטגית</u>? אלו התומכים בגישת ה'עוד מאותו דבר' (more of the same) רואים בסייבר כלי נוסף בארסנל האסטרטגי הקיים ל'שכנוע בכוח' (coercion) או ללוחמה חסויה/חשאית. לכן גם אין מקום לדבר על 'מלחמות סייבר' כמושג עצמאי. מוקדם מלדעת אם לכלי זה תהיה השפעה גדולה יותר על שינוי מדיניות אצל היריב (כלומר, שיהא אפקטיבי יותר מכלים אחרים בראייה אסטרטגית). עמדה זו אף מצדדת בהותרת החוק הבינלאומי ללא שינוי ושימוש בו גם לצרכי סייבר.

למול זה יש לשאול: (1) מדוע הקימו פיקוד סייבר אלמלא ראו בסייבר עניין אסטרטגי ייחודי?[1] (2) באלו הקשרים יכולים מאפייניו הייחודיים של כוח סייבר לפתח פוטנציאל אסטרטגי שלא היה קיים אחרת עקב מגבלות פיזיות או לגיטימיות? ו-(3) כיצד יתקבל טיעון זה במעבר מספקולציות סייבר לחק"בי? (כשהשכיחות תעלה...)[2].

(2) <u>הקבלה בין המימד הקינטי למימד הקיברנטי</u> - או הויכוח בין אלו המצדדים בעמדה שהסייבר אינו מימד לחימה נפרד (warfighting domain)[3], לבין אלו הרואים פוטנציאל חדש אופרטיבי ואסטרטגי הנובע משונותו של מימד זה ביחס למימדים האחרים[4], בין אם כפעולה מתחת לסף (סביבות חשאיות/ חסויות) ובין אם כפעולה מנטרלת אך לא קטלנית (סביבות מערכתיות - הגיון המהלומה). להחלתה או דחייתה של הפריזמה הקינטית על ענייני הסייבר השפעה מכרעת בין היתר על האסטרטגיה האמריקאית ואופן הפעלת הכוח; ועל המסלולים החוקיים (דומסטית וגלובלית) המעניקים לגיטימציה להפעלת הכוח (למשל, קידום אמנות בינלאומיות חדשות ייחודיות למלחמות סייבר או מתיחת החוק הבינלאומי הקיים של עימות מזויין ואמנות הומניטריות).

ג'ייסון הילי[5], מאלו המחזיקים בדעה שהסייבר משקף או מותח מציאות קיימת, טוען שיש להכפיף את העימות בסייבר לכללי העימות המזויין הקיימים דווקא משום שזהו מרחב אזרחי בראש ובראשונה ואזרחים ומערכות אזרחיות פועלים בו ומוטמעים בו. מלחמה קינטית מתנהלת top-down ונמצאת, בעיקרון, מחוץ ליומיום האזרחי[6], בעוד שמלחמת סייבר מתנהלת bottom-up וכחלק מחיי האזרחים. לכן, יש לחדד את האבחנה של המותר והאסור בו שבעתיים עבור מדינות, ובאמצעות החוק

---

1. הערתו של ז.ג.
2. יוזמת הסייבר בראשות ג'ייסון הילי שבמועצה האטלנטית, עומדת להוציא לאור בשנה הקרובה מחקר על ההסטוריה של עימותים בסייבר, הגם שלא זכתה לשיתוף פעולה ישראלי באיסוף הנתונים...
3. כמו מרטין ליביקי: http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf, 2012 "Cyberspace is not a Warfighting Domain"
4. ראו מאמרו של ד"ר עמוס גרנית, *Cyberspace as a Warfighting Domain - In What Way?* המל"ן, 2012.
5. Jason Healey, Director - Cyber Statecraft Initiative, Atlantic Council
6. אזרחי ישראל בעידן מלחמות הטילים יטענו אחרת...

הבינלאומי הקיים. ככל שעימות מתקרב לאזורים האסטרטגיים המסורתיים, כך גדל הסיכוי לכלול בתוכו גם פעולה סייברית.

נעשית כאן הבדלה בין מעשי מדינות מחוץ לנורמות/ מוסכמות של עימות גלוי או מלחמה קינטית (סדירה, המגובה באמנות האו"ם והרשאותיו) כמו נוזקות מסוג stuxnet (אליהם הוא מתנגד) לבין מלחמה על סוריה שתחל במתקפה סייברית לשיתוק מערכות הגנ"א, אותה הוא רואה כלגיטימית. כלומר, דווקא המדינות ה'אחראיות' צריכות להוביל קו העושה שימוש גלוי בסייבר תוך לקיחת אחריות מדינתית לאקט, לבין השימוש החסוי בו. וגם אז, צריך לשכנע את העולם שהשימוש בסייבר נעשה כדי שהמלחמה תהא פחות קטלנית.

* מקרה-מבחן ה-Flame[7]: האישור לכאורה שנתן הממשל האמריקאי לעשות מניפולציה מכוונת על מוצר אזרחי כדי לפעול נגד יריביו בסייבר, משול להפיכת מוצר אזרחי של חברה עסקית לנשק! במובן זה, הילי טוען שפעולה זו היתה החלטה של אנשים במדים (קהיליית המודיעין) מתוך מחשבה לטווח קצר, המערערת את המערכת ונמצאת מחוץ לטווח הלגיטימיות. בהקשר זה, ניתן לראות במתקפן מאיראן על מערכת הבנקאות האמריקאית כתגובה לתולעת סטקסנט, אך משמעה שאלו הנפגעים מהפעלת אגרוף סייברי הם המגזר העסקי או האזרחים[8].

חברי-הצוות לחקיקה וביטחון לאומי בלשכת עורכי-הדין האמריקאית, שמילאו תפקידים בכירים בממשל בתחומים הללו ומציגים עמדה ניצית בסוגיית הסייבר, טוענים שהשיח הקיים באמריקה על מלחמה ושלום מגביל מבחינה חוקית את היכולת לקיים ביטחון לאומי, ואינו עוזר לחשוב על אסטרטגיה מאחר והוא דיכוטומי - משול למתג ON/OFF - בעוד שבמציאות ישנו "מרחב ניבזי" שמתחת לסף ההסלמה (nasty space shy from escalation). לכן, הציווי האסטרטגי הראשון שיאפשר פעולה יזומה בהיבט החוקי שלה הוא היכולת לזהות את התוקף - ומכאן - שהיכולת המשלימה הנדרשת לפעולה היא היכולת המודיעינית להטיל אחריות (attribution). מאידך, יש צורך לשרטט קו בין שימוש בתוכנה או בתקיפת תוכנה כדי לממש אפקט קינטי, לעומת השימוש בחוק הקיים של עימות מזויין לאותה מטרה, ושוב - כדי להגדיל את מרחב הפונטציאל האסטרטגי.

(3) <u>עיצוב כללי המשחק האסטרטגיים (סייבר והחוק הבינלאומי)</u>: ארה"ב רואה עצמה מובילה נורמטיבית גם בסייבר - אך דווקא כאן מדובר בגורם מחשק ולא מדרבן - ראשוניות התקיפה המדינתית (המוצהרת) בסייבר גוררת מטען פוליטי או רגישות פוליטית לכל החלטה, לא רק של הפעלת כוח אלא גם של פיתוח יכולות. מכאן נובעת גם העיכוב בהוצאה לפועל מתקפת סייבר יזומה.

באמנה הקיימת, ישנה אבחנה בין שימוש בכוח (use of force) לבין התקפה מזויינת (armed at-tack). בהקשר סייברי, הסוגייה המשפטית המשמעותית ביותר קשורה להיעדר זיקה גיאוגרפית מסורתית שהיתה מסייעת בהגדרת גבולות אחריות או סמכות. כלומר, יש ניתוק בין הזיקות זמן-מרחב, מאחר והסייבר אינו מרחב גיאוגרפי ומבצעי הסייבר וירטואליים, ואל-זמניים. מצב זה גורר קובעי-מדיניות לחשוב (בטעות כמובן) שיהיה להם זמן לקבל החלטות בעידן הסייבר על סייבר, למרות שבפועל, לא יהיה להם זמן אפילו למצמץ...

מאידך, הסייבר דורש נקיטת גישה <u>פרו-אקטיבית</u> מאחר ובשונה ממימדים אחרים בהם הכלים (הגנריים) קיימים ומאפשרים סגירת מעגלים מהירה יחסית, בסביבה הסייברית לוקח שנים לפתח

---

7. שימוש בפירצה בקוד של עדכוני מיקרוסופט כפתח להחדרת נוזקה. ראו: http://securitywatch.pcmag.com/microsoft-windows/298622-microsoft-revokes-certificates-used-by-flame-malware

8. http://www.themarker.com/wallstreet/1.1832313

כלים לאיסוף ותקיפה אך מעבר לזה - הכלים חד-פעמיים משתי סיבות: האחת - השונות המהותית בין המערכות; השניה - ברגע שהכלי נחשף, אי אפשר להשתמש בו שוב. כלומר, סייבר דורש התייחסות אחרת לזמן האסטרטגי - נדרשת היערכות ממושכת, מתמדת ויזומה, למול אפסיות זמנית במונחים של החלטה על פעולה.

צריך להיות זרז כדי להוציא לפועל מתקפת-סייבר מדינתית (מכת-מנע) אך הזרז אינו חייב להיות סייברי בעצמו. בוש הבן קבע במפורש דוקטרינה של מכת-מנע בכהונתו, הגם שהנשיא אובמה לא מסר הצהרת המשך. כרגע משתמשים בז׳רגון של הרתעה בהקשרה הסייברי.

מהו אפקט סייבר? אין עדיין דוגמא בעימותי-סייבר לאפקט ארוך-טווח. יש דוגמאות לאפקטים נקודתיים עם הרס רב (סטקסנט), או אפקטים רוחביים עם הרס זניח (מתקפות DDOS)... עד שמגיעים לאפקט קינטי ונזק פיזי, לא נחשב חלק ממשטר החוק הבינלאומי (לגיטימציה, מידתיות, הפללה - legitimacy, proportionality, discrimination). כל עוד הנזק לא מוחשי (מאחר ואינו פיזיקלי) וקשה להעריכו, לא ניתן להפעיל את החוק. דוגמא: אסטוניה מול אראמקו - במתקפה הרוסית על אסטוניה 2007[9] לא היה נזק ישיר, ולכן לא היה שימוש לכלי המשפט הבינלאומי; בסעודיה היה נזק פיזי ל-30 אלף מחשבים, ועל ניתן ליישמם. כלומר, ניתן להחיל את החוק הבינלאומי הקיים גם לתוך מבצעי הסייבר.

הגישה האמריקאית המקודמת באמצעות מחלקת המדינה מציבה סייבר כנשק הומניטרי (לא קטלני) וכנשק הפיך (reversible).

* נשאלת השאלה מדוע האיראנים לא פנו לאו״ם ודרשו זכות תגובה לגיטימית משנתגלתה תולעת סטקסנט? התשובה קרוב לודאי מאחר ולא היתה זו התקפה מזויינת (armed attack) אלא שימוש לא חוקי בכוח (use of force), והצידוק היה עמום מדי.

** מהו האפקט המערכתי ההופך ריגול לנזק אסטרטגי? והיכן עובר הקו בין ריגול (חוקי מוסקבה) לבין גניבת נכסים אינטלקטואליים מוגנים? (פשיעה מוכרת בחוק)?

=> המסקנה היא שהמטריה המשפטית אינה בשלה עדיין לקדם את החשיבה על הפוטנציאל האסטרטגי בשימוש בכלי סייבר ואינה מקדמת את החשיבה המבצעית - לכן צריכה להיפתח בשלב מאוחר יותר וכמאפשרת, לא כמגבילה! מאחר ויש עדיין מקום רב לפרשנות של כללי המשחק. הסוגייה המשפטית הבאה על מערכה בסייבר, תעסוק באבחנה בין מודיעיני לצבאי, ובין חסוי לגלוי.

(4) שיחים אנלוגיים לסייבר - מול גרעין (הקבלה בין השיח הגרעיני של שנות ה-50 לשיח הסייבר של שנות ה-2000)[10], הנובעת מסימני שאלה מהותיים לגבי חומרת האיום שסייבר מציב בהקשר המדינתי, וגוררת בין היתר הימנעות משימוש במינוח ׳התקפה׳ בהקשר ההפעלתי (no first use) לטובת מושגים השאולים משיח המגננה (כמו ׳הגנה פעילה׳ active defense) או ב׳מאזן עוצמה׳ וי׳כולת השמדה הדדית׳; או, סייבר במנעד שבין לוחמה סדירה ללא סדירה - בניסיון לברר מהי לוחמת סייבר, נעשות הקבלות לסמלים בהסטוריה הצבאית (cyber Dunkirk, cyber Vietnam, הקרב על בריטניה...). יש הטוענים כי השימוש במינוחים של לוחמה לא-סדירה משרת אפקטים סייבריים נכון יותר.

---

9. http://www.ynet.co.il/articles/0,7340,L-3419525,00.html

10. http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/

(5) מהו איום הייחוס? ייחשב 'פרל הרבור' בסייבר? (ראו נאומו של מזכיר ההגנה פאנטה לאחר מתקפת הסייבר על חברת האנרגיה הסעודית, אראמקו, 15 אוגוסט 2012[11]). מאחר והעולם עוד לא חווה מלחמת סייבר בין-מדינתית באופן מפורש ומקרי-המבחן בהם נתקפו מדינות בסייבר עדיין מועטים וחלקיים, יש מקום נרחב לספקולציות, הגם שאלו משפיעות באופן ישיר על המוטיבציה המדינתית להתארגנות אסטרטגית בסייבר ועל קצב המימוש שלה. יש קולות הטוענים כי בעשור האחרון הסקטור הפרטי/ מגזר עסקי הפסיד טריליוני דולרים כתוצאה מגניבה של מידע מסחרי ואינטלקטואלי, שהביא לסגירת מפעלים ולאובדן מקומות-עבודה. במובן זה, 'פרל הרבור' כבר קרה!

החידוש במתקפה על אראמקו היה בנזק הפיזי הישיר שגרם וירוס "שאמון" לעשרות-אלפי מחשבים ולדאטא של חברת האנרגיה הסעודית, לעומת מתקפות מבוזרות של מניעת-שירות (DDOS) שגורמות נזק תדמיתי יותר מאשר מוחשי וברות-התאוששות מהירה. לכן מהווה מתקפה זו מקרה-מבחן משמעותי לחשיבה על סייבר ברמה האסטרטגית, הגם שקיימת סברה שאיראן בחרה להשבית את החברה המספקת תחליף לנפט האיראני עבור המערב כתגובה לסנקציות שהושתו עליה.

התרחישים הנחשבים מאיימים ברמה הלאומית קשורים לשחקנים מחוץ למרחב האמריקאי, שנשלחו לפגע על ידי יריב מדינתי או שמעשיהם מגובים על ידי יריב מדינתי. שר ההגנה פאנטה שירטט בנאום 'פרל הרבור' את איום-הייחוס כמתקפה שתגרום נזק פיזי מסיבי ואובדן חיים, תהמם את האומה ותשתק אותה ותיצור תחושת פגיעות חדשה: מדינה מתעמתת או קבוצה קיצונית שישתלטו על מערכות SCADA[12], יסיטו רכבות נוסעים או כאלו המשנעות משא לא-קונבנציונלי ממסילותיהן, יזהמו את מקורות המים בערים הגדולות, יורידו את רשתות החשמל, ויעשו זאת בו-זמנית ובשילוב עם מתקפה קינטית. התוקפים עשויים לנטרל או לפגוע במערכות צבאיות/ תקשורת קריטיות.

ויקיליקס כארוע משנה מציאות: תופעה סייברית שנבעה מביזור צינורות-המידע והיעדר השליטה בהם במובן הטכני/ כמותי/ נוהלי, אבל השפיעה אסטרטגית על היחסים הדיפלומטיים של המעצמה הגדולה בעולם ושינתה את האופן בו מתפקדת מחלקת המדינה מאז.

(6) פרדוכס מידת הקידמה כמידת הפגיעות: עליונותה של ארה"ב הטכנולוגית/ סייברית גוררת בקרב רבים מסוכני השיח הנחה א-פריורית של היותה הפגיעה ביותר בסייבר מקרב המעצמות; סיבה נוספת לתחושת הפגיעות האמריקאית נובעת מסגנון הפעולה הקואליציוני והצורך לשתף ברשת שחקנים בינלאומיים בעלי יכולות סייבריות נחותות, מה שעשוי להוות פירצה/ חולשה במערכת.

(7) מיהו היריב? עדיין נתפש במונחים וסטפאליים (מדינתיים). במובן זה, פיקוד הסייבר רואה בסין את היריב המשמעותי בעיניים אמריקאיות מאחר ורוב הנזק הכלכלי הסייברי מקורו ביוזמות סיניות. פרשנות מתחרה רואה בסינים כרודפים אחרי אמריקה במירוץ הפיתוח הסייברי (עמק הסיליקון). כלומר, גם תחושת הפגיעות ולא רק פוטנציאל הנזק, הדדיים. בשני המקרים וללא מנגנוני 'בירור' או הסדרה בין-מדינתית, עלולות מעצמות אלו למצוא עצמן נוקטות בפעולה בוסרית שלא התכוונו לה. בהקשר זה, תחת אכסניית מכוני-המחקר ישנם דיבורים תמידיים עם הסינים, בעיקר כדי להזהירם

---

11. http://www.washingtonpost.com/leon-panetta-warns-of-cyber-pearl-harbor/2012/10/13/6cdcbd6e-14c9-11e2-9a39-1f5a7f6fe945_video.html
ורקע על המתקפה עצמה: http://www.themarker.com/wallstreet/1.1849442

12. Supervisory Control and Data Acquisition - מערכות מתוקשבות לשליטה וניטור של תשתיות קריטיות, תעשיות ומפעלים, ושכיחות בתחום האנרגיה.

מפני חישוב מוטעה (באנלוגיה לפרל הרבור וההפצצה הגרעינית על יפן...). מאידך, הסינים טוענים שלא יתקיפו את וול סטריט כי הם המשקיעים העיקריים בבורסת ארה"ב והראשונים שייפגעו מכך...

עם זאת, ברור כי בעידן זה, לצד המשך של יריבויות מסורתיות באמצעים אחרים (סייבריים), נוצרו גם יריבויות מסוג חדש (גניבת הון אינטלקטואלי לרמה של קריסת תעשיות) ומצד שחקנים לא מדינתיים (אנונימוס, האקרים פטריוטיים...).

(8) <u>הפללה (attribution) ו/או היכולת לממש 'הרתעה' בסייבר בהיעדר היכולת לזהות את היריב</u> - משרד ההגנה, כמדיניות, אינו משתמש ב'שליחים' (proxies) בעימות מזויין[13], כדי לשמר שליטה בהתהוות. יריבותיה של ארה"ב לעומת זאת (רוסיה, סין, איראן) אינן בוחלות בכך. מכך נגזרת העמדה האמריקאית לגבי אחריות מדינות למתקפות סייבר היוצאות משיטחן (third-party). הסינים מאידך (וכהשלכה של ההיגיון הפוליטי/ תרבותי שלהם) רואים בכל מתקפה היוצאת מטריטוריה בשליטה אמריקאית ככזו שזכתה לגושפנקא מהממשל - מה שעשוי להביא לכך שיוזמות פרטיות לפעולה בסייבר (למשל, גופים אמריקאים המבצעים מתקפה בסין כדי לתמוך במתנגדי ממשל, או חברות אמריקאיות המגיבות כנגד מתקפה סייברית מסין), יתדרדרו לעימות בין-מדינתי מבלי שהתכוונו לכך...

במסגרת אישור תקציב הביטחון לשנת 2011, דרש הסנאט ממשרד ההגנה לענות על 13 סוגיות הקשורות למדיניות הסייבר של הממשל[14]. בין היתר, נדרש משרד ההגנה לבאר את המשמעות של אימוץ עמדת הרתעה בסייבר, כשאין יכולת לזהות את היריב מחד, וכשאין כוונה (בשלב הזה) לעשות 'הדגמת יכולות' גלוייה מאידך.

(9) <u>דיפלומטיית סייבר - מחלקת המדינה</u>: סייבר נדון גם כסוגייה על-מדינתית. מדינות צריכות להתארגן כדי להגן על עצמן, אך גם הקהילה הבינלאומית צריכה להתארגן כדי להגן על עצמה. יש צורך בנקיטת צעדים מעשיים תוך הימנעות מעירבוב אידיאולוגי בדינמיקה שבין הסדרה ומשילות.

בשנים 2009-10 נשעה מאמץ דיפלומטי בינלאומי[15] להתוות צעדים בוני-אמון בין השחקנים המדינתיים, שיכפיפו באופן ראשוני את הפעולה המדינתית בסייבר לחוק הקיים. הסוגיות העיקריות היו היכולת להטיל אחריות והצורך למנוע חישובים מוטעים (attribution, miscalculation). לאורך כל הדרך וגם כיום, גוש המדינות האלטרנטיבי (non-aligned countries) מתנגד למהלך הזה ורוצה חקיקה ייחודית לסייבר.

שנים קודם לכן, עסק האו"ם בהובלת סוכנות ה-ITU[16] בקידום אמנות נגד פשיעה סייברית (פורנוגרפית ילדים, גניבת כרטיסי אשראי, קופות רושמות...) אך כיום מנהלות את ה-ITU מדינות

---

13. בגדול, מתקיימת אבחנה תחת מבצעים שבהובלת משרד ההגנה (צבא/ סדיר/ לוחמה רגילה) תחת סעיף 10, לבין מבצעים שבהובלת ה-CIA (לוחמה חסויה/ חשאית/ ריגול...) תחת סעיף 50. ראו: http://www.dtic.mil/dtic/tr/fulltext/u2/a494716.pdf

14. Department of Defense Cyberspace Policy Report, Nov. 2011, Section I:
http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf

15. הנציגה הישראלית בשיחות היתה השגרירה רודיקה רדואן-גורדון, כיום מכהנת במקסיקו.

16. International Telecommunications Union - במקור עסק בחלוקת תדרים גלובלית והתגלגל לעסוק ברגולציה של טכנולוגיות ותקשורת. כמו גופים אחרים באו"ם, לא מובל כיום על ידי המערב ועוין במהלכים שלו להשקפת-העולם הליברלית).

כסוריה ואיראן. המנכ"ל הנוכחי הנתמך על ידי הסינים, עושה שימוש בארגון מלזי המקושר לקספרסקי לשם קידום נהלי אבטחת-מידע ומטרתו לקדם שליטה בסייבר שאינה טכנית אלא תכנית - כמכשיר לרגולציה של מדיניות ציבורית. כמו כן, הסוכנות מובילה קו שימנע גישה חופשית וחינמית לאינטרנט בעולם, הן מסיבות אידיאולוגיות (בהיותו כלי המאפשר ערעור סדרים פוליטיים וחברתיים), והן מסיבות כלכליות (בהמשך למודל מרכזיות הטלפוניה, מקדמות 'עמלה' על תעבורת אינטרנט)[17].

ארה"ב אינה שולטת אם כן נכון לעכשיו בהכתבת אמנה מוסכמת ואינה נתפשת כמובילה, אלא כמתחרה עם סין, רוסיה ובנות-בריתן האוטוריטריות על עיצוב הנורמות במרחב. חלק מהקושי להגיע לנורמות בינלאומיות מוסכמות נעוץ בכך שהאיחוד האירופי איבד את מעמדו באו"ם לעומת מעצמות חדשות שיש להתחשב בהן, דוגמת ה-BRIC, מדינות דרום-אסיה, טורקיה ומדינות אפריקה, המקדמות ציר אלטרנטיבי למערב. ממשלים אלו עסוקים בראש ובראשונה בהבטחת שרידותם ורואים במדיה החברתית כלי המאיים על יציבות השלטון (מה שהתחוור בבירור ב'אביב הערבי' או בשימוש שנעשה כיום ברשת הסקייפ בקרב כוחות האופוזיציה בסוריה, עד כדי כך שמדינות כמו מצרים וסוריה ניתקו את האינטרנט במדינה בניסיון להקשות על יכולת התיאום של ההתנגדות).

מאידך, היעדר היכולת לייצר משילות בסייבר (מדינתית ובין-מדינתית) עשוי להביא למצב שלא נוכל לפעול במרחב. לכן, המאבק הדיפלומטי על עיצוב האמנות נע בימים אלו בין שלושה מימדים: לגיטימציה לניטור מדינתי בתכנים שברשת; לגיטימציה לגרימת נזק למערכות סייבר או באמצעות מערכות סייבר; ובאופן המופשט יותר, שליטה באינטרנט (בהבדלה ממערכות סייבר).

עם זאת, גם ארה"ב כנושאת הדגל של חופש הביטוי, עברה תזוזה מעמדה אידיאליסטית (בנאום הסייבר הראשון של אובמה, הבטיח שארה"ב "לעולם לא תנטר את האינטרנט..." כקו אדום מבחינתו) לדיבור על איזונים.

מכאן, שאין כרגע תשובה טובה למתח שבין יצירת סביבה בטוחה בסייבר, לבין הקרבת ערכים דמוקרטיים ליברליים (כחופש הביטוי או הזכות למחאה). במובן המינימלי, חותרים להסכמות בדומה למלחמה הקרה כמו 'חוקי מוסקווה' (40 הדיברות למרגל המתחיל...) של עשה ואל תעשה.

(10) מיליטריזציה של מרחב הסייבר ישנו מתח מובנה בהקשר הסייברי בין האינטרסים של הממשל, לבין האינטרסים של האזרחים, לבטח כל עוד מירב הפעילות במרחב הסייבר נעשה על ידי המגזר הפרטי. מתח זה משתקף בדיון על המיליטריזציה הגוברת של מרחב הסייבר, בשלושת המימדים: איסוף, הגנה והתקפה. מהצד האזרחי/ העסקי, ישנה קריאה נאיבית-נואשת להפסיק את 'הכיבוש' או לכל הפחות, לקדם יתר שקיפות של הפעולות הממשליות או בלית-ברירה להשקיע יותר בפוזיציה הגנתית (פיתוח של מערכות הגנתיות על פני יכולות תקיפה).

חברות התקשורת (Telecommunication) האמריקאיות-גלובליות, יוצאות על כן מנקודת-מבט הפוכה לזו של הממשל: הגדרת האינטרסים שלהן כוללת שמירה על שלמותה של הרשת, וידוא שהלקוחות העסקיים והמוסדיים מקבלים מענה לצרכיהם הייחודיים (בנקאות, תעשיות), ווידוא שלאנשים הפרטיים יש גישה מובטחת לרשת (בפנאי ובחירום). בראייתן, הרשת היא נכס שהן יצרו, בונות ומתחזקות אותו. לטענתן, הגברת המעורבות הממשלתית בסייבר תיתן לגיטימציה להמשך המיליטריזציה של המרחב ולהרחבת העימות המדינתי המסורתי לתוכו. ולהיפך - שמירה של מרחב סייבר 'מאוזרח' תעקר את הלגיטימציה לפעול בו צבאית ותגן בעקיפין על האזרחים או הפעילות

---

17. להרחבה ראו: "דמיינו שמורידים את השאלטר של האינטרנט" - http://www.ynet.co.il/articles/0,7340,L-4316439,00.html

האזרחית במסגרתו (פרטית, ציבורית, חברתית, כלכלית). במלים אחרות, המיליטריזציה של מרחב הסייבר מזיקה ללקוחות ולמשתמשים מאחר והיא גוררת מירוץ חימוש שפוגע לא רק ב'מדינה', אלא בישויות שהמהות שלהן סייברית.

כמו כן, ובניגוד להגיון הפעולה המדינתי, לחברות עסקיות או מערכות אזרחיות הנפגעות בסייבר, זהות התוקף אינה רלבנטית ליכולת להתגונן, אלא סוג הפגיעה. במובן זה, אנונימוס, סין או איראן - חד הם. לעומת זאת, לשם מניעה או התגוננות מפני מתקפות סייבר יש משמעות לדיון בזהות היריב וזהו המקום בו המערכות האזרחיות והממשליות-צבאיות חייבות למצוא דרך להיפגש.

בעיניים מפוכחות, המרחב הסייברי הפך צבאי כבר לפני שני עשורים (הפיצוץ בצינור הגז הטרנס-סיבירי 1982 כתוצאה מהתערבות במערכות הפעלתו, המשוייך ל-CIA), כביטוי להרחבה הבלתי-נמנעת של ריבונות מדינתית. לכן, כל שנותר לעשות הוא למסד את מגרש-המשחקים ואת כלליו.

כיצד מתארגנים להגנה מדינתית בסייבר?

מרחב הסייבר הבטחוני התהווה מתוך תחומי-תוכן של ריגול, האזנות, הצפנה ופיענוח. מבחינה מוסדית היה על-כן על מה להישען, הן מבחינת התפישה, והן מבחינת הפרישה והמערכות, ההכשרה וכוח-האדם. ה-NSA, ארגון הביון הממשלתי וסוכנות הסיגינט הלאומית שהוקם בשנת 1952, היתה ועודה הישות הדומיננטית בהובלת ההתארגנות הבטחונית-מדינתית לפעולה בסייבר[18] (והעומד בראשה מפקד גם על פיקוד הסייבר). במובן זה, יש הרואים בפיקוד הסייבר התהוות טבעית מתוך המתפתחות המימד, ולא כורח חדש.

עם זאת, וככל שמתחוור הכורח בעירוב המגזרים הממשלי הלא-בטחוני, העסקי והפרטי על מנת להיערך לאיומי הסייבר, עולות שאלות ערכיות, חוקתיות וארגוניות אשר לחלוקת הסמכות והאחריות (פיקודית ומקצועית) וסדר-העדיפויות. בהקשר זה, ישנם מתחים מהותיים:

(1) בין הממשל (וה-DHS הנחשב כשלוחה הבטחונית שלו) לבין משרד ההגנה;

(2) בין הישויות השונות בתוך משרד ההגנה על הגישות המובחנות/ התמחותן בסייבר;

(3) בין הממשל לבין חברות התקשורת וספקיות האינטרנט (האחראיות מסורתית לאבטחת-מידע של מערכות התקשורת האזרחיות והאינטרנט כנכס הקנייני שלהן);

(4) בין הגישה הרפובליקנית לדמוקרטית בגבעת הקפיטול - סביב סוגיות רגולציה, פיקוח ופרטיות.

<u>"הקשר הישראלי" - נקודת המפנה בהתארגנות המדינתית</u> בארה"ב היתה "solar sunrise"[19] - מתקפה שהוביל אהוד טננבאום (ה'אנלייזר') על מחשבי משרדי ההגנה בשנת 1998. המבוכה היתה כפולה מאחר ולא היה ברור עמד מאחרי הפעולה (יריב מדינתי, שחקן בודד...) ומאידך, לא היה ברור

---

18. על תתי-המערכות שלו. לדוגמא: DISA - Defense Information Systems Agency - גוף בן 50 האמון על ייצור מעטפת סייבר תומכת מבצעים ולחימה למערכת הביטחון וסוכנויות המודיעין (בין היתר ניטור של מערכות משרד ההגנה, הקמת רשת המידע הגלובלית GIG - Global Information Grid, או קיום נציגויות בפיקודים המרחביים והזרועות: www.disa.mil

19. ראו כתבה וסרט הכשרה של האף.בי.איי: http://www.wired.com/threatlevel/2008/09/video-solar-sun/

מי אחראי לטפל בה במערכת. כתגובה, יצרו במשרד ההגנה כוח משימתי משולב, ישות שהתפתחתה וגדלה בהתמדה לרמת פיקוד של גנרל 2 כוכבים. ככל שגבר הצורך בתיאום עם סוכנויות אחרות, הוחלט לבסוף להקים פיקוד נפרד משודרג לרמת גנרל 4 כוכבים (CYBERCOM).

<u>מהן נקודות-המבט המעצבות מדיניות/ הסדרה של השוק האזרחי בהיבט ההגנתי</u>? (אינטרנט/ קהילה, עסקים, ממשל) - מטריצה בטחונית (פנים-מדינתי) ובטחונית-צבאית (חוץ) בשלושה מעגלים:

(1) ניטור האינטרנט - רמה בסיסית (המטפלת ב 80-85% מפגיעות רשתות נגועות או Bot-nets[21]): שימוש בספקי האינטרנט להגנה על לקוחות ומשתמשים פרטיים;

(2) תשתיות קריטיות - יידרשו 20 שנה נוספות לשדרג את התשתיות. רובן מפגרות ברמת התיפעול/ הגנה אחרי ההתפתחויות הסייבריות;

(3) הגנת המדינה - בשיח האמריקאי היתה עד לא מזמן מחשבה שאין לצבא תפקיד בהגנה בסייבר על המדינה ועל כן אינו מחוייב לפיתוח שלושת היכולות הנדרשות (איסוף/ מודיעין, הגנה/ אקטיבית, התקפה יזומה). גופים וסוכנויות אחרים במשרד ההגנה עוסקים בכך שנים ארוכות בהתפתחות הטבעית של תחומי-הידע והטכנולוגיות הנלוות להן, הגם שסייבר כנשק נחשב עניין חדש יחסית - בשלבי פיתוח תפישות וצורות יישום. בהיבט הגילוי והניטור, ישנה הקבלה מסויימת בין NORAD[21] לבין CYBERCOM - כפיקוד המנטר את מרחב הסייבר. המדיניות המוצהרת היא שלמשרד להגנת המולדת קדימות חוקתית מעל משרד ההגנה מבחינת האחריות להגנה קיברנטית על המדינה (DHS over DOD) והוקם בו לאחרונה חפ"ק האמור לתכלל את מאמצי ההגנה במערכים האזרחיים[22].

<u>הגנת המדינה - מקומו של פיקוד הסייבר במערכת</u>:

משרד ההגנה עדיין בעיצומו של תהליך ניסוח מדיניות כאמור, שתאפשר 'ליהנות' מההזדמנויות האסטרטגיות הטמונות בעוצמה האמריקנית המגולמת במימד הסייבר. בהקשר הפנים-מדינתי, נדרשת אבחנה בין האינטרנט (כיישות מסחרית בגדול) לבין מרחב הסייבר בכללותו. החוק הקיים מטיל מגבות משמעותיות על פעולה דומסטית של הצבא בסייבר, הגם שיש אינדיקציות שהנשיא העביר באוקטובר 2012 תיקונים לחוק[23] שיאפשרו פעולה של סוכנויות משרד ההגנה בהקשר המקומי גם מחוץ למנדט הנוכחי (הגנה על מערכותיו ומתקניו של המשרד, כולל מתקני הצבא, בסיסיו, כוחותיו ומבצעיו). בהקשר זה, נאום 'פרל הרבור' של מזכיר ההגנה פאנטה, נועד לתת הד ציבורי למהלכים

---

21. בוטנט הוא אוסף של סוכני תוכנה (software agents) או רובוטים אשר רצים באופן אוטומטי. המונח נפוץ בהקשר לתוכנות נוזקה (Malware, Malicious software). כמו כן, בוטנט מתייחס לרשת של מחשבים שמריצים אפליקציה שיודעת לעבוד עם פקודות שמתקבלות דרך האינטרנט. האפליקציה רצה בצורה עצמאית ואוטומטית, מה שמאפשר שליחה של פקודות מרחוק לכל הרשת. ראו: http://www.yedatech.co.il/yt/keyword.jhtml?value=3168

21. North American Aerospace Defense Command - הפיקוד האמריקאי-קנדי המנטר את שמי המדינות והחלל מפני תקיפות למיניהן מהאוויר: http://www.norad.mil/about/index.html

22. NCCIC - National Cybersecurity and Communications Integration Center. ראו: http://www.dhs.gov/about-national-cybersecurity-communications-integration-center-nccic

23. http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story_1.html

מאחרי הקלעים להרחבת סמכויות משרד ההגנה גם למרחב האזרחי. מאידך, גם סוכנויות הביטחון מבינות שעליהן להיפתח לסוכנויות האחרות ולשחקנים האזרחיים במרחב הזה. ב-NSA מדברים כיום על שיתוף מידע בזמן אמת, אך עניין זה נופל בין הכסאות הסוכנותיים והיריבות המסורתית ביניהם. לכן, מנסים כרגע לקדם את שיתוף המידע על ידי הפיכתו ל'אנונימי' - למרות שאז משלמים בחלקיות שלו. זאת, בחתירה למצוא איזון בין הדרישה לפרטיות, לבין הדרישה לביטחון.

פיקוד הסייבר שהוקם בשנת 2010, התפצל מתוך STRATCOM - המושך הגרעיני ריכז בו ריבוי של אנשי-מודיעין וטכנולוגים מהמובילים בתחומים, שעם תום המלחמה הקרה היו זקוקים ל'הסבה' או לתכלית מחודשת.

היעד המיידי והראשי של הפיקוד להגן על מערכות משרד ההגנה. עדיין מתנסים בהפעלתו גם כתומך מערכות סייבר שיובלו על ידי הפיקודים הלוחמים, וגם כנתמך במשימות גלובליות שיוביל בעצמו (supporting /supported). הפיקוד אחראי לגייס, לאמן ולצייד את מרכיבי הסייבר בשירותים ובמפקדת הג'וינט. כיווני ההתפתחות שלו, מלבד בניין-כוח והכשרה, כוללים את הסינכרון של פעילות קיברנטית בין הפיקודים השונים והפעלת כוח עצמאית.

החיבור של CYBERCOM ל-NSA בסידור הפיקודי נועד כדי לתת לו את הגב הסיגינטי, את הסמכות המקצועית ואת האמצעים ליישם את ייעודו. כדי לסבר את האוזן, בנתונים הנוכחיים, הוצאת הפיקוד מה-NSA תצמצם את יכולותיו ב-70%! מה גם שהרגולציה החדשה אמורה להעניק ל-NSA סמכויות נוספות להגן בפני או לעצור מתקפות בסייבר.

<u>פיקוד הסייבר נמצא בתווך (ובמתח) שבין ישויות המודיעין לישויות המבצעיות</u> ועדיין מחפש את עצמו: "Cybercommand is a snapshop in a movie in progress". מאחר ולא השקיעו את האנרגיה האינטלקטואלית בבירור הזה, נוח לפיקוד לעבוד כרגע תחת המטריה ה'חסויה'. עם זאת, ככל שהוא מזוהה יותר כ'מודיעיני', הוא מתקשה להשתחרר מהצל של ה-NSA. ככל שהוא מזהה עצמו יותר כגוף אופרטיבי, הוא נדרש למצב עצמו ביחס לרכיבי הסייבר בפיקודים המרחביים ובזרועות האסטרטגיות, שלחלקם (כמו ל STRATCOM ולזרוע האווירית) הסטוריה ארגונית ארוכה עם התחום (ולכל הפחות, עם חלק ממימדיו - צופן ופיענוח, תיקשוב וכו').

סיבה נוספת לכך שפיקוד הסייבר משייך עצמו קרוב יותר לצד המודיעיני של ספקטרום התיפקוד, כדי לחמוק מהרדאר המשפטי - בהמשך ל'חוק הג'נטלמני' קובע כי "לא מדברים על מבצעי מודיעין/ ריגול במסגרת החוק הבינלאומי".... (לעמדה זו שותפה במידה רבה גם מחלקת המדינה, כתחום שעדיין חומק מהסדרה בהקשר האו"מי).

<u>יחסי-הגומלין בין ה-NSA לבין CYBERCOM</u>: מה העוצמה של פיקוד צבאי ברגע שמתייגים אותו כזרוע מודיעינית, וכשהוא נבלע בתוך ישות מודיעינית ענקית?... מנקודת-מבט מודיעינית, כל פעולה בסייבר משמעה איבוד נכס מודיעיני-איסופי (מה שמהווה את ההצדקה לקיומם raison d'etre); לעומת זאת, אנשי מבצעים יחשבו קודם על המשימה ואחר כך על איך למזער את הנזק המודיעיני. במילים אחרות - אנשי מודיעין רוצים להשיג מודיעין מבצעי, רק לא רוצים לצאת אחר כך לפעולה בעקבותיו... (Actionable intelligence without the Action...).

הבעיה היא שבסייבר, הפלטפורמה אחידה גם להשגת מודיעין וגם להפעלת כוח. לכן, יש הטוענים שזו היתה טעות אחת למקם את פיקוד הסייבר תחת ה-NSA, וטעות שנייה, לשים עליהם מפקד אחד בשני כובעים! (כיום תחת גנרל קית' אלכסנדר). סידור זה היה יכול להיות אפקטיבי יותר לו הישויות הפיקודיות היו זהות במעמדן/ משקלן - או אז, היה מתפתח ויכוח אינטלקטואלי אמיתי בין אנשי-המודיעין, לבין אנשי-המבצעים.

בגלל הסידור הפיקודי הנוכחי, מפקדי הזירות המרחביות (המוציאים לפועל את מבצעי הסייבר), לא יודעים מספיק על סייבר כדי להתמודד שווה בשווה עם DIRNSA (NSA Director) - כדי להתווכח על מהות המבצעים ודרך הוצאתם לפועל.

כמו כן, אין עדיין לפיקוד הסייבר כוח סייבר שיספק לפיקודים המרחביים רכיבי סייבר שווי-ערך ביכולותיהם לרכיבי הזרועות האחרות (אויר, יבשה, צי, מארינס...). בפועל, עושים כיום רגולציה להכשרות לוחמי סייבר (cyber operators) בזרועות השונות, ואף אינם אחראים לממן אותן.

בחלוקה לסוגי היריבים/ האיומים, השחקנים הלא-מדינתיים אינם נחשבים מתקדמים דיים להוות איום ממשי בסייבר (לבטח בראייה צבאית) ועל כן לא מטופלים על ידו. ריגול, מאחר ומוכוון על ידי מדינות, מטופל לא על ידי הפיקודים הזירתיים, אלא נמצא באחריות הפיקוד ובתוקף סמכותו החוקית והביצועית - היכולת לעצור של זליגת מידע וכסף מחוץ לגבולותיה הריבוניים של ארה"ב (extract or disrupt transfer of money or knowledge).

סין ורוסיה נחשבות בעיות החורגות מיכולות הפיקוד ועל כן מטופלות בשילוב ה-NSA וה-CIA.

חוסר-בהירות לגבי בעיות סייבר במרחב הפיקודים הזירתיים: סין למשל משוייכת בחלוקה הגיאוגרפית לפיקוד הפסיפי. התגוננות מול סין או התקפתה במרחב הזירתי של PACOM, תיעשה בהובלת מפקד הפיקוד, כש CYBERCOM תומך. לעומת זאת, פעולה של סין במרחב הלאומי האמריקאי מטופלת על ידי הפיקודים הלאומיים (NSA, CIA, CYBERCOM). נשאלת השאלה, היכן מסתכנרנים המאמצים הללו ובאחריות מי? זהו מרחב העמימות שעדיין ממתין להסדרה תפישתית, ארגונית ופיקודית הן במרחב הפנים-מדינתי והן בהקשר החוץ-מדינתי.

<u>תשתיות קריטיות</u>: 85-90% מהתשתיות הקריטיות בארה"ב נמצאים בידי המגזר הפרטי. גם תחום הסייבר (והאינטרנט), בראייה הסטורית, צמח בארה"ב במגזר הפרטי (מבחינת השקעות, פיתוח תשיות ומוצרים והגנה עליהם).

המערכת המדינתית נמצאת עדיין בסטטוס תגובתי ביחס לצורך להגן על תשתיות קריטיות מפגיעות סייבר (הגם שלאורך השנים, פותחו עבורן תפישה להגנה מפגיעות קינטיות), ונדרש עדיין שכנוע רב בצורך לעסוק בפיתוח תחום זה וכתיבת תפישה עבורו.

אנרגיה - חברות החשמל הינן התחום המתקדם ביותר בהסדרת SCADA, חברות המים והגז מפגרות בהתאמה לסביבה החדשה. מדובר בריבוי של סוגי מיכשור, תוכנות ותהליכים ורק לשם המחשה, יש לזכור שבארה"ב למעלה מ-3,000 חברות המייצרות חשמל ומספקות אותו במדינות השונות... עם זאת, מה שקשה להסדרה, לתיקנון ולתיאום, קשה גם להתקפה - הפרדוכס הוא שהן גם מחוסנות יותר כתוצאה מהשונות/ יתירות הזו (diversity). כלומר, אפשר לעשות נזק נקודתי - גם אם משמעותי - אך לא מערכתי/ הסטורי/ משנה מציאות אסטרטגית לאומית.

מגמות המשפיעות על ההגנה הסייברית של מערכות SCADA:

א. המתח/ פרדוכס בין חיזוק ההגנה על ידי ניטור /מיערוך/ קישוריות, לבין יצירת פגיעות חדשה. בעבר הושגה בטיחות בעמימות (security by obscurity). היום אין יתירות לחומרה/ לתוכנה - יש firewall אחד בשוק למערכות SCADA...

ב. רוב המפעלים המייצרים את המערכות הללו אינם אמריקאיים...

ג. גם ההתקדמות לאנרגיות ירוקות/ מתחדשות מייצרת בעקיפין חולשה חדשה - מאחר ואלו מבוססות על התייעלות של המערכות, מעודדות שליטה, ניטור ותיאום מרחוק (למשל מערכות smartgrid לניהול רשת החשמל), בין אם לצרכי חסכון, תחזוקה או אבטחה.

ד. לכן, הדרישה העכשווית בפיתוח היא לנהל מאמצים מקבילים של התייעלות לצד אבטחה.

מעבדת המחקר לניהול סיכונים בהגנת סייבר[24], בראשה עומד ד"ר ג'ון סאונדרס (מומחה עולמי למערכות SCADA), פועלת תחת ה-(Chief Information Officer) CIO של משרד ההגנה וה-J6 ומהווה בעמדה זו צינור להעברת ידע וממצאים לרמה הלאומית. המטרה - לייצר קפיצת מדרגה בחשיבה על בעיות הגנת סייבר של מערכות אלו ברמה הלאומית, ואלו יכולות נדרשות על מנת להגן עליהן. במובן זה, המעבדה הינה חוד החנית הלאומי של העלאת המודעות להגנה על מערכות SCADA. מעבר להיותה גוף מחקרי, המעבדה הינה הגוף המוביל בהכשרת סוכנים מדינתיים (כולל אנשי צבא) ומספקת הסמכה להגנה על מערכות אלו - מערכות השליטה לסוגיהן (אנשים, פיזיקה, תוכנות) וסוגי תקיפות פוטנציאליות. הקורסים נעשים בשיתוף החברות הפרטיות המייצרות את המערכות ומפעילות אותן. כמו כן, למעבדה יש מערך הכשרה נודד (מעין דגם מוקטן של המערכת) אותו ניתן לשנע לפיקודים המרחביים למטרות הכשרה.

<u>ניטור האינטרנט ואבטחת-מידע</u>: ספקיות האינטרנט האמריקאיות מהוות כיום חלק מחברות תקשורת גלובליות. במובן זה, ראייתן משלבת את המימד התוך-מדינתי (והאמריקאי לצורך העניין) למימד הבינלאומי (התשתיות שלהן חוצות גבולות ריבוניים ולחלק מהחברות בעלות לא-אמריקאית). חברות אלו טוענות, מעבר לזכות הקניין על הרשת, לעמדה מקצועית ולידע רב יותר על אופן הפעולה ברשת וחולשותיה, לעומת הרשויות המדינתיות, מאחר ואלו הן שעיצבו ובנו את הרשתות.

כיום ישנם מאות מיליוני משתמשים באינטרנט המעבירים ביניהם טרה-בייטס של דאטא יומיומית. אין יכולת לנטר את התעבורה הזו באופן שרירותי. רוב ההתקפות עד היום לא כוונו כנגד רשתות התקשורת עצמן אלא כנגד הלקוחות. מבחינת החברות, הביטים העוברים ברשת הם נייטרליים (קומבינציות של 0,1). תרבותית, לא ינטרו תנועה של ביטים כדי להגן על הפרטיות. חוקית, אסור להן לנטר - רק הלקוח יכול לבקש זאת מהחברה, עד כדי חסימת תנועה של דאטא. אם הממשלה מגדירה סוג של ביטים כ'רעים', חברות התקשורת יכולות למנוע תעבורה כזו. אבל נדרשת הוראה רוחבית, גורפת, ובאישור משתמשי-הקצה.

לכן, הן דורשות כיום מהממשל שיתוף במידע מראש על איומים אפשריים (advanced threat) כדי שיוכלו להתכונן אליו. בהמשך הדרך, הן רואות בסוג כזה של מידע מודעיני שירות שיירד לרמת מוצר אזרחי/ פרטי אותו יספקו כחלק מחבילת השירותים שהן מוכרות.

מכאן נגזר הדיון ב'אבטחת-מידע' - האם זהו מצרך ציבורי, פרטי, או יתרה מזו - מצרך לשם רווח? (מוצר) נפיצות נושא זה מצויה בטענת הממשל כי החברות אינן יכולות/ רוצות/ לא רווחי להן להעניק שירותי אבטחה ראויים בסייבר, ולכן יש כשל-שוק בתחום זה. חברות התקשורת טוענות מצידן כי הממשלה כובלת את ידיהן ומייצרת את העיוות בשוק במו ידיה, ואז מייצרת רגולציה היכן שאינה מחוייבת המציאות. זאת משום שאין כיום בשוק דרישה לאבטחה ברמה גבוהה יותר (ברמת

24. DoD Cyber Defense Risk Management Lab, חלק מה-iCollege ב- NDU

המשתמש) ועל כן אינן מפתחות מוצרים כאלו (ברמת הספק). עם זאת, ברור להן שהמעבר ל'ענן' מייצר בעיה מסוג חדש, משום שעכשיו לא מדובר רק באבטחת תנועה של ביטים, אלא באבטחה של מידע (מעובד, מאוחסן). לכן, ייאלצו להגביר את רמת האבטחה וסוגי אבטחה שהן יספקו. זוהי אינה מחלוקת עניינית גרידא ויש לה מקורות-הגיון כלכליים-פוליטיים. על כך יורחב בפרק העוסק בגבעת הקפיטול בהמשך.

רגולציה: השיח האמריקאי נסב על מתן או מניעה של סמכויות הסדרה ואכיפה לבית הלבן והממשל הפדרלי, הן כחלק מתפישת-עולם כוללת הקשורה בחירויות-הפרט מול הממסד, והן משיקולים מעשיים - כמו יכולות הסוכנויות להוציא זאת לפועל טוב יותר מכוחות השוק, יכולות מקצועיות של הסוכנויות (החדשות בעיקר) להקים ולהפעיל מערך הבנוי משמעותית על הבנה טכנולוגית מתקדמת, וההשלכות על תהליכים כלכליים שייפגעו מכך. באופן גס, המחלוקת חוצה את הקונגרס והסנאט על הקווים המפלגתיים המסורתיים - הרפובליקנים והדמוקרטים חלוקים ביניהם על מידת המעורבות הממשלתית בסייבר ועל מי להטיל את האחריות הפדרלית הנגזרת, באופן המשקף את מחלוקת-העל הערכית/ פילוסופית/ פוליטית על מידת מעורבות פדרלית בחיי האזרחים, בכל התחומים.

הקהילות המדעית והכלכלית המצדדות באינטרנט חופשי וחינם (בצד הערכי והיזמי) הינן בעלות משקל רב בממשל אובמה. עם זאת, הן מתעלמות מהמציאות האסטרטגית העכשווית מאחר וערכים אלו משלו לפני 15 שנה. כיום, גוף הרגולציה הגלובלי הדומיננטי (ITU) פועל בסתירה לכך כאמור ומאותם טיעונים, רק כתמונת ראי שלהם (מאבקי כוח פוליטיים/ אידיאולוגיים ושיקולים כלכליים).

המצדדים באכיפה פדרלית בתחום הסייבר (דמוקרטים) טוענים כי המגזר הפרטי אינו משקיע מספיק בהגנת התשתיות הסייבריות וחד היא אם מסיבות כלכליות או מחוסר-ידע מקצועי כאמור. הרפובליקנים מצידם מובילים קו (אותו הם מנסים להעביר בוועדת הכוחות המזויינים ובוועדה העוסקת במסחר ומדע), הקורא להגדיר נורמות מומלצות - אך לא מחייבות - ולהביא למצב בו יש שיתוף וולונטרי במידע. במלים אחרות, הרפובליקנים קוראים בראש ובראשונה לשיתוף במידע, ואם לא יביא לתוצאות הרצויות, להמשיך לרגולציה ואכיפה. מהן המשמעויות?

1) סוכנויות ההגנה הלאומיות יידרשו להוריד את רמת הסיווג של מידע מודיעיני ולהפיץ אותו למגזר הפרטי; מצד שני, חברות האבטחה וספקיות השירותים האינטרנטיים/ סייבריים יצטרכו לחלוק את החולשות שלהם בסייבר והתקפות שחוו הלקוחות שלהם, כמו גם לאפשר ניטור עמוק יותר של תנועת-המידע על התשתיות שלהם; מצד שלישי, האזרחים יצטרכו להתרגל לכך שלא כל הפרטיות שלהם מוגנת.

2) רגולציה לרוחב המערכות הפיננסית והצרכנית, עשויה לפגוע בקשרי ספקים-לקוחות (חוסר אמון מצד הלקוחות בחדירה לפרטיות, מה שיפגע בכלכלה בכלל; שת"פ מידע שיתרחב לא רק לעניינים בטחוניים, אלא להתנהלות לא-חוקית של הלקוחות בתחומים אחרים...).

- שאלת האחריות הפדרלית לרגולציה - מאבק בין הסוכנויות: יש המצדדים במתן הסמכות והאחריות להגנה בסייבר בידי המשרד להגנת המולדת, כדי לשמור על פרטיות האזרחים. המתנגדים טוענים שמשרד זה לא הצליח להתרומם מקצועית באף אחד מהתחומים שגולגלו אליו, סובל מכוח אדם בינוני ומביורוקרטיה מיותרת. בהקשר הסייברי, אין ספק שהידע הטכנולוגי שלהם נחות ביחס לסוכנויות בטחון אחרות. אלו המצדדים במתן הסמכות למשרד ההגנה, רואים בהגנה בסייבר חלק מביטחון לאומי כולל ולכן, צריך לשבת ב-NSA וב-DOD. הממשל הפדרלי יכול, בדומה ל-FDA, להעניק 'ציונים' למאמצי אבטחה של המגזר הפרטי (מבחן התוצאה), אך לא לאפנן אותה מראש (להגדיר תהליך מסויים).

* בעיניים ישראליות, יש לזכור כי למשרד ההגנה האמריקאי אחריות רק כלפי עובדיו ומתקניו ואין לסוכנויות שלו רשות אכיפה פנימית, כלפי האזרחים (סמכות זאת ניתנת רק לרשויות הפדרליות כמו ה-FBI וה-DHS). כלומר, אם יהיה שינוי כזה שישית אחריות להגנה בסייבר עליו, יצטרכו לשנות זאת בחקיקה.

3) <u>הסייבר מרחיב בצורה דרמטית את מעגל האנשים שיצטרכו לעבור רגולציה</u>. לכן, המשרד שתינתן לו סמכות זו ברמה הלאומית, צריך להיות כזה עם ניסיון רב לא רק בסייבר, אלא ברגולציה גרידא (לשם השוואה, ה-FDA אחראי לרגולציה של מזון ותרופות עשרות שנים. ה-DHS בקושי מצליח לעשות רגולציה לאסונות-טבע...). יש להיזהר מכך שחקיקה רעה תפגע ביכולות האבטחה הקיימות. כמו כן, יש סכנה שאם חברות פרטיות יידעו שמגיעה רגולציה, ולוקח שנים לאפיין אותה, הן יפסיקו לפתח מוצרים על שום החשש שלא יעמדו בתקן בסופו של דבר. זו תהא פגיעה נוספת בלקוחות ובתהליכים הטבעיים של מחקר, פיתוח, ייצור ושיווק.

4) <u>שאלת האחריות המדינתית בתחום הסייבר בעידן של פעילות עסקית גלובלית</u>, כשרוב חברות הטלקומוניקיישן והאינטרנט הינן חברות גלובליות או מקומיות, הפרושות על פני הגלובוס - כיצד עושים רגולציה חוצת-גבולות? על מה מגינים? עד כמה ניתן להרחיב את המנדט הזה? הרפובליקנים חוששים שסין למשל תשתמש בהרחבת הרגולציה כדי לפגוע בפעילות של חברות זרות בשטחה, או לחילופין, לפעול לגיטימית בארצות זרות כדי להגן על חברות סיניות.

5) מבחינה פוליטית, הסייבר לא נחשב עדיין חומר פוליטי <u>חם</u> ונדון במסגרת הוועדות המקצועיות. הבית הלבן וה-DHS דוחפים לרגולציה דרך הוועדה העוסקת בתחומי-שיפוט (jurisdiction), כדי לייצר ריכוזיות בתחום שיתוף-המידע אצלם. כיום עוסקות בכך 7 ישויות נפרדות! ריכוזיות על כן משמעה מתן עוצמה פוליטית ופיקודית בידי גוף אחד.

* <u>מי מיועצי הנשיא דוחף 'שליטה על האינטרנט'</u>?? מאחר ולא מדובר רק ברגולציה של סייבר, אלא גם ברגולציה של האינטרנט, שנחשבת שיאה של האנושות החופשית/ מערבית. הרפובלקנים רואים בכך סדין אדום...

מגמות תרחישיות בהתפתחות מרחב הסייבר והגנתו

- האינטרנט מתפרק (בלקניזציה של האינטרנט) - ישנן רשתות נפרדות מקבילות, סוג של מלחמה קרה (סין, ארה"ב, רוסיה...). רשתות אלו יתחרו גם בערכים המגולמים בהן.
- המרחב האינטרנטי הופך להיות מרחב צבאי בהגדרתו (בדומה לטלגרף) - עצירת הקידמה - מה שיביא להתהוות של סידור טכנולוגי/ תקשורתי חדש שיחליפו.
- הידרדרות מתקפת האקרים פטריוטיים להסלמה קינטית של עימות שנוהל/ נשלט עד כה בין מדינות (הודו-פקיסטן, ארה"ב-סין...)
- חישוב מוטעה (miscalculation) של מכה מקדימה סייברית - האם ייתפש בעיני היריב כתחילת מתקפה (שלב מקדים לקינטי) או כצעד מניעתי (דוחה מתקפה קינטית)?

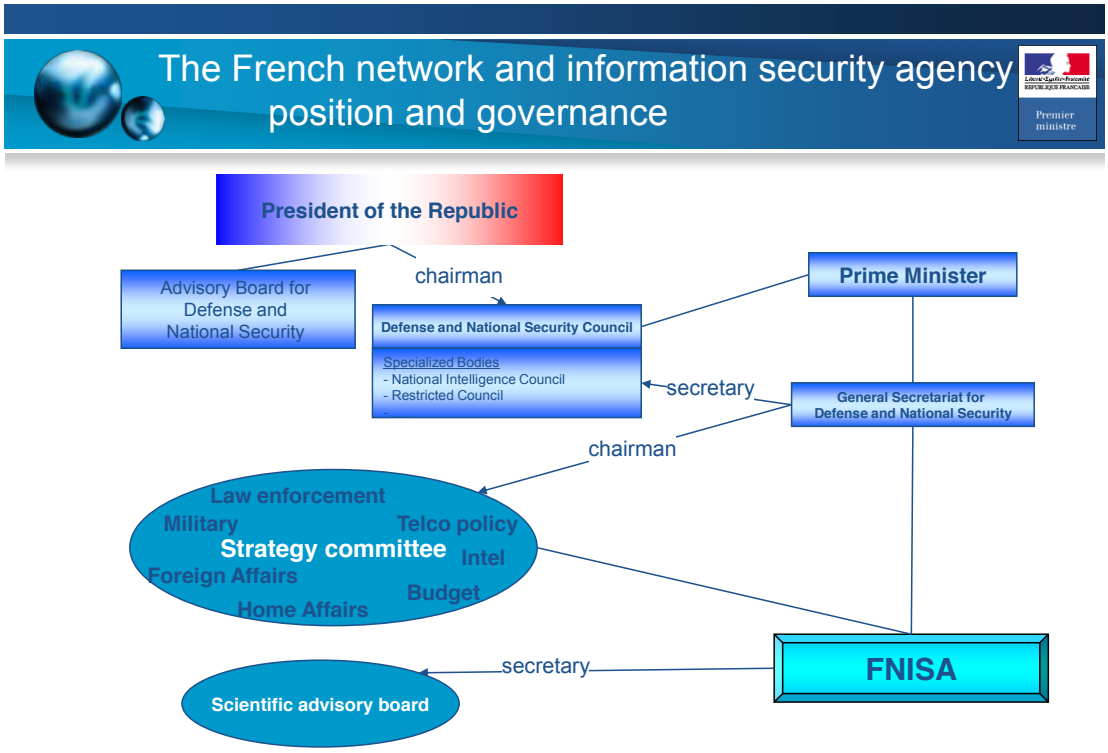
מה ניתן להקיש מהמקרה האמריקאי להקשר הישראלי?

- חופש-פעולה אסטרטגי בסייבר: במידה מסויימת, ידיה של ארה"ב כבולות יותר מאשר ידיה של ישראל מאחר וארה"ב רואה עצמה כמכתיבה נורמות גלובליות.
- 'דילמת המגן' - ניתוח שרירותי נטול הקשר של איומי-ייחוס ('פרל הרבור') עשוי להעמיד את מפעל ההגנה המדינתית כסיזיפי במיוחד. עם זאת, כשמבררים את צרכי ההגנה בהקשר אסטרטגי ייחודי, הגבולות 'ברי-הגנה', הגם שיש לתאם את המאמצים הללו עם מאמצי התקיפה והאיסוף במקביל, ולא כפועל יוצא של המערכה.
- בישראל תאימות הדוקה יותר בין המגזר הפרטי לבין המגזר המדינתי/ לאומי, לטוב ולרע - אין לנו ריבוי ספקים ושחקנים בהקשר הרגולטורי, אך במקביל, הופך כל שחקן כלכלי גדול במערכת לבעיית אבטחה לאומית, גם אם מדובר בחברה בבעלות פרטית (בזק, תנובה, בנק הפועלים...).
- ההיערכות ההגנתית המדינתית במרחב הסייבר מצריכה שילוב של ראייה פנים-מדינתית עם חוץ-מדינתית ולאומית עם גלובלית (צורך בשת"פ בינארגוני הן דומסטית והן בפעולה מחוץ לגבולות המדינה). בשתיהן אין לישראל ניסיון רב. בימים אלו מועלות הצעות אלטרנטיביות של המטה הקיברנטי הלאומי, צה"ל והשב"כ להסדרה של הפעולה בסייבר, לאישור הממשלה[25].

---

25. בהקשר זה הוצע לבחון את המודל הצרפתי לניהול סייבר ברמה הלאומית ANSSI, כמתאים יותר לצרכים ולהקשר הישראלי:

http://www.ssi.gouv.fr/en/



- האם פני ההגנה המדינתית בסייבר צריכות להיות אזרחיות (משטרה...) או בטחוניות/ צבאיות? מאחר והסייבר/ אינטרנט נתפשים ככלי-ביטוי של חברה חופשית, התערבות או נוכחות-יתר של מערכת הביטחון נתפשה בארה"ב כצורמת במיוחד. עם זאת, יש לקחת בחשבון את האמון של הציבור באותן מערכות - בישראל, נהנה צה"ל מתמיכה עצומה, אך זו נשחקה כשהופעל בהקשרים 'אזרחיים' (כמו ההתנתקות).

- סוגיית הרגולציה מטרידה מאד את האמריקאיים, אך כמעט ואינה נוכחת בתרבות הישראלית... נגיעות ראשונות בכיוון ניתן לראות בויכוח המתנהל בשולי האקטואליה אשר למאגר הביומטרי[26] ובצורך לאזן בין הדרישה לפרטיות לבין הדרישה לביטחון ולשתף את המגזר העסקי והאזרחי במידע ובהיערכות אקטיבית להגנה בסייבר.

- אפקט הסייבר - סייבר כהשתקפות של התרבות הנוכחית וכמרחב של נוחיות בעיניים אזרחיות - אפליקציות, פרופילים (אקזיסטנציאליסטי, גניבת זהות...), סידורים ויומיום, קשר עם הרשויות הממשליות, סוציאליזציה חברתית, מקור-המידע המוביל... במובן זה, הנזק הסביבתי שיכול להיגרם כתוצאה ממתקפה יזומה בסייבר על 'העורף', עשוי להיות קשה יותר לעיכול מאשר מלחמת טילים...

- הכשרה לסייבר - העמימות ביחס לפוטנציאל הקיים במימד ולאופן בו הוא משנה את הביטחון הלאומי. ההכרה כי מרחב הסייבר הופך את פירמידת-הידע (הצעירים מתקדמים הרבה יותר מהותיקים וחיים את העידן הטכנולוגי); העכבות הפסיכולוגיות בכל הקשור לקידמה טכנולוגית ולסוג העיסוק ה'וירטואלי' או המופשט יותר; הקושי באיתור סוכני-ידע ובעלי-ניסיון ברמה המדינתית; הצורך ללמד בצורה אחרת, ההולמת את המימד (אינטראקטיביות, קישוריות, זמינות, המחשה)[27].

---

26. ראו ריכוז כתבות בנושא המאגר ומתנגדיו: http://www.ynet.co.il/home/0,7340,L-7752,00.html

27. BYOD, BYOE – bring your own device, bring your own environment - חניכים/ סטודנטים מורגלים בסביבה אותה הביאו מהבית/ מהחיים ובממשק (אינטרפייס) שבין העיסוק האונטולוגי לקיברנטי.