



פרסומי מרכז דדו

1/2016

סקירה 1 בנושא הסייבר סוגיות אזרחיות הנוגעות לפעולת המדינה במרחב הסייבר -

שמואל שמואל

פברואר 2016, שבת התשע"ו

שמור

תקציר

מרחב הסייבר הוא מרחב חדש וייחודי. ככזה, הפעולה האנושית בו מביאה עימה מגוון סוגיות עבור המדינה. סוגיות אלה נוגעות לאופי פעולת המדינה במרחב הסייבר, למידת פעולתה בו, לדרך פעולתה בו ולגבולות האחריות והסמכות שלה ושל סוכנויותיה בכל הנוגע למרחב הסייבר. בעת זאת, כשאר הולכות ומתהוות התפיסות הבסיסיות של המדינה למרחב הסייבר, קיימת הזדמנות ייחודית למצוא פתרונות מקיפים ויסודיים למגוון מהסוגיות שהוזכרו לעיל. באם לא ימצאו פתרונות מוסדרים ומקיפים, יהיה על המדינה לפעול בשיטת כיבוי שרפות וניהול משברים – דרך יקרה יותר ויעילה פחות.

המאמר שלהלן נועד לסייע לצוות גיבוש התפיסה של מדינת ישראל למרחב הסייבר. בתוך כך, למרות שנכתב בצה"ל, יתרחק המאמר מהעיסוק בנושאים הצבאיים במרחב הסייבר וידון בחלק מהסוגיות ה"אזרחיות" יותר הנוגעות לפעולת המדינה במרחב הסייבר. מטרת המאמר היא בעיקר להעלות סוגיות לדיון והוא אינו עוסק במציאת פתרונות לסוגיות אלה.

סקירה זה היא חלק מסדרת סקירות בתחום שמטרתם לפתח את הידע הבסיסי הקיים ולהעשיר את המפקדים וקציני המטה העוסקים בתחום.

תוכן עניינים

4	מבוא
6	המקורות שבשימוש המחקר
6	קווים כלליים בנוגע לאבטחת מרחב הסייבר ברמת המדינה
8	סוגיות מרכזיות בפעולת המדינה במרחב הסייבר
8	חלוקת סמכויות בין המגזר הפרטי לממשלה
15	חקיקה, נורמות, רגולציה ותקנון
22	תיאום
23	שיתוף מידע
29	בניין כוח – פיתוח ידע, הכשרה, כוח אדם וארגון
34	סיכום
38	נספח א' – שאלות למחקרים נוספים
39	בבליוגרפיה

מבוא

מרחב הסייבר חיוני במידה הולכת וגדלה לאורח החיים במערב ולתפקודים הולכים ומתרחבים של החברה האנושית. ההגדרות המדויקות למרחב הסייבר אינן מוסכמות עדיין על הכל, אך עם זאת, אפשר לדבר על מרחב זה כ"העצמים המסתמכים או מתבססים על טכנולוגיית מחשבים ותקשורת, המידע בו עצמים אלה משתמשים, מאחסנים, מנהלים או מעבדים והאופן בו עצמים אלה מקושרים בניהם". בהתאם, אבטחת מרחב זה מוגדרת כטכנולוגיות, תהליכים ומדיניות המסייעים למנוע או לצמצם את ההשפעה השלילית של אירועים במרחב הסייבר, העשויים להתרחש כתוצאה מפעילות מכוונת נגד טכנולוגיית המידע על ידי שחקן עוין.¹

מרחב הסייבר שונה מהמרחבים הפיזיים בין השאר בכך שהוא מרחב שעצם קיומו נובע מפעולה אנושית. בשונה מהאוויר, הים, היבשה והחלל החיצון, אין מרחב סייבר בהיעדר בני אדם (וטכנולוגיית המידע שהם המציאו ומתחזקים). באופן כללי, כיוון שמרחב הסייבר הוא מרחב חדש, עדיין לא ברורות סוגיות שונות הקשורות לפעולה בו. מקובל לחשוב, בהקשר זה, שבדומה למרחבים הפיזיים, גם במרחב הסייבר מוטל על הממשלה להגן על האינטרסים הלאומיים, על צרכי האוכלוסייה, על המשק ועל שגרת החיים במדינה. עם זאת, חלקו של המגזר הפרטי במרחב הסייבר גדול מאוד ולא ברורה חלוקת האחריות בינו לבין הממשלה בכל הנוגע להגנה על מרחב זה.² הדגש הניתן לאחריותה של המדינה במרחב הסייבר (ובמיוחד בהגנה עליו), נוטה להסיט את הדיון, באופן טבעי, לסוגיות הביטחוניות והצבאיות הנוגעות לפעולת המדינה במרחב הסייבר. עם זאת, הסטה זו באה לעיתים על חשבון דיון מקיף בסוגיות אזרחיות, שחשיבותן רבה.

לפיכך, נדרש בירור מעמיק יותר של מספר סוגיות עקרוניות הרלוונטיות לפעולת הממשלה במרחב הסייבר ולתפקידיה במרחב זה. המאמר שלהלן ינסה להעלות מספר סוגיות פתוחות בפעולת המדינה במרחב הסייבר, כפי שאלה מופיעות בחלק מהספרות הגלויה כיום. לא מדובר ברשימה מלאה או ממצה של הסוגיות הקיימות והקורא יוכל בנקל לחשוב על סוגיות רבות נוספות שלא נידונו במאמר זה. עם זאת, מדובר בסוגיות שהעיסוק בהן נרחב יותר מאשר אחרות. בתוך כך, יש לזכור שלרבות מהסוגיות הללו אין עדיין פתרון היום. לכן אפשר שהמאמר יעלה בעיקר שאלות, אך לא יישא בשורה בתחום התשובות. כמו כן, מכיוון שבפרסומים הגלויים נידון בעיקר הפן ההגנתי של לוחמת הסייבר, יעסוק המאמר כמעט אך ורק בהיבטים

¹ David Clarck, Thomas Berson and Herbert S. Lin (eds.), **At the Nexus of Cybersecurity and Public Policy – Some Basic Concepts and Issues**, Washington, DC: National Academies Press, 2014, p. 1

לדיון מעמיק יותר בנוגע להגדרות מרחב הסייבר ראה:

יוסי הוכבאום, "המרחב הקיברנטי – הגדרתו, קווים לתפיסת המבצעים במרחב וארגון הפיקוד על ניהולם על פי המודל האמריקני", בתוך: אמ"ץ-תוה"ד, **המרחב הקיברנטי (הסייבר)**, תצפית 61, אפריל 2011, ע"מ 66-7

² לדיון בעניין זה: שמואל אבן, "אסטרטגיה לשילוב המגזר הפרטי בהגנת הסייבר הלאומי בישראל", **צבא ואסטרטגיה**, כרך 7, גליון 2, INSS, ספטמבר 2015, ע"מ 89-105

שמור

הגנתיים אלה. על ידי הדגשת הסוגיות שאינן צבאיות-ביטחוניות הנוגעות לפעולת המדינה במרחב הסייבר, אמור המאמר לסייע לגיבוש תפיסת הסייבר.

המקורות שבשימוש המאמר

המאמר ישתמש בשני סוגי מקורות עיקריים:

1. אסטרטגיות הגנה בסייבר של ארה"ב ושל האיחוד האירופי.
2. מחקרים אזרחיים הנוגעים לפעולת המדינה במרחב הסייבר ולסיכונים במרחב זה.

שני סוגי מקורות אלה משלימים האחד את השני. המחקרים האזרחיים מציגים מגוון אתגרים הקיימים במרחב ומציעים להם פתרונות ואילו האסטרטגיות הרשמיות עוסקות בעיקר באופן בו המדינות מנסות להתמודד עם מגוון הסוגיות המדוברות במחקרים האזרחיים. שילוב של מקורות אלה מאפשר לעמוד, באופן כללי, על מגוון הנושאים המעסיקים את המדינה בכל הנוגע לפעולותיה במרחב הסייבר ועל האופן בו היא מתכוונת לטפל בנושאים אלה.

קווים כלליים בנוגע לאבטחת מרחב הסייבר ברמת המדינה

באופן כללי ההגנה במרחב הסייבר אינה קשיחה, אינה מוחלטת ואינה בהכרח צבאית. בהינתן הפגיעות המובנית של מרחב הסייבר והאימונים השונים הקיימים בו, מטרת האבטחה במרחב הסייבר היא לאו דווקא למנוע לחלוטין פריצות והתקפות במרחב זה, אלא לוודא שטכנולוגיית המידע מתפקדת כמו שצריך, למרות הפגיעות הנרחבת והמובנית שלה.³

באופן כללי, אפשר לסווג את הפעילויות לשיפור האבטחה במרחב הסייבר לשני סוגים עיקריים כדלהלן:⁴

- שיפור האפקטיביות של האמצעים הקיימים.⁵
- מחקר של ידע ואמצעים חדשים.⁶

שיפור האפקטיביות של הגורמים הקיימים אינה סוגיה טכנית בעיקרה, כי אם ארגונית, משפטית, הכשרתית וכו'. כך לדוגמה, לעיתים כדי לשפר את אבטחת המידע בארגון מסוים, אפשר לשפר את נהלי אבטחת המידע, להקל על שיתוף המידע בתוך הארגון ובינו לבין לגורמים אחרים (פרטיים או ממשלתיים), להכשיר טוב יותר את כוח האדם בו וכו'. מנגד, מחקר ידע ואמצעים חדשים ויישומם הם כן סוגיות טכניות וטכנולוגיות בעיקרן.⁷

³ David Clarck, Thomas Berson and Herbert S. Lin (eds.), **At the Nexus of Cybersecurity and Public Policy – Some Basic Concepts and Issues**, Washington, DC: National Academies Press, 2014, pp. 19, 22

⁴ *Ibid*, *Op. cit.*, p. 2

⁵ לדוגמה – שיפור נהלי השימוש בטכנולוגיה קיימת או שינוי החקיקה הנוגעת לה כדי לשפר את האפקטיביות שלה.

⁶ המצאת טכנולוגיות ופיתוח אפליקציות חדשות.

⁷ David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, p. 2

כיוון שהאיומים במרחב הסייבר הם מגוונים מבחינת השחקנים, יעדיהם, השיטות בהן הם משתמשים והמטרות שהם תוקפים, מתן מענה לאיומים במרחב הסייבר אינה סוגיה הנתונה לאחריותה וסמכותה הבלעדיות של המדינה וזאת ממספר סיבות.

ראשית, מכיוון שהמדינה אינה שחקן ניטראלי ונטול אינטרסים בנושא. המדינה מנצלת את מרחב הסייבר לצרכיה ואלה לא תמיד עולים בקנה אחד עם הצרכים והאינטרסים של גורמים אחרים הפועלים במרחב. מעבר לכך, לעיתים, אפשר שלמדינה יהיה אף אינטרס מובנה לשמור על פגיעות מסוימת של מרחב הסייבר כדי להקל על מאמצי האיסוף והתקיפה במרחב זה.⁸ כמו כן, בדומה לכל נושא אחר, למדינות שונות יהיו אינטרסים שונים במרחב הסייבר, בין השאר בהתאם ליכולות התקיפה וההגנה שלהם במרחב זה, לפגיעותם בו ולאיומים עליהם (לדוגמה יכולות היריבים שלהם והאזרחים שלהם).⁹

לא זו אף זו, באופן כללי (והדבר משתנה לפי חוקי המדינה), לעיתים מוגבלת המדינה מלטפל באיומים במרחב הסייבר באופן ישיר. כך, לדוגמה, מנועים מוסדות המדינה מלפעול באופן חופשי במערכות תקשוב שונות, לדוגמה כאלה השייכים לאזרחים וארגונים אחרים למיניהם – במיוחד בזמן שגרה. בהתאם לעיתים קשה למדינה להשתמש ביכולות צבאיות או צבאיות-למחצה במרחב הסייבר האזרחי המקומי (ובמקרים מסוימים – גם החוץ מדינתי).¹⁰ מכאן שמקומם של הכוחות המזוינים בכל הנוגע לאבטחת מרחב הסייבר קטן מאשר מקומם באבטחת המרחבים הפיזיים והמענה לאבטחת מרחב הסייבר אינו עניין צבאי טהור, אלא מאמץ הכולל את כל גורמי הממשל (Whole of Government) ואף את החברה כולה.¹¹

⁸ לדוגמה, אחד מגילויי פרשת סנאודן הייתה שסוכנות ה-NSA הכניסה כשלים מובנים ומכוונים בהצפנות שעזרה לפתח כדי שתוכל לפרוץ אותן בעצמה. ראה:

Peter Bright, "Report: NSA Paid RSA to Make Flawed Crypto Algorithm the Default", **Ars Technica**, 21 Dec. 2013,

www.arstechnica.com/security/2013/12/report-nsa-paid-rsa-to-make-flawed-crypto-algorithm-the-default/; Peter Bright, "The NSA's Work to Make Crypto Worse and Better", **Ars Technica**, 6 Spe. 2013, www.arstechnica.com/security/2013/09/the-nsas-work-to-make-crypto-worse-and-better/;

כמו כן, חלק מסוכנויות הממשל האמריקני תומכים כעת בניסיונות להעביר חקיקה בקונגרס שתכניס "דלת אחורית" בכל הצפנה שתפותח בארה"ב. ראה:

Dustin Volz, "FBI Director: Encryption Is Great As Long As It Lets Us In", **Defense One**, 6 Jul. 2015, www.defenseone.com/technology/2015/07/fbi-director-encryption-great-long-it-lets-us/116998/

⁹ David Clarck, Thomas Berson and Herbert S. Lin (eds.), **Op. cit.**, pp. 70-71

¹⁰ עם זאת, פיתוחים טכנולוגיים מקלים כיום על זיהוי אירועים חריגים במרחב הסייבר גם ללא חדירה למידע אישי. שמואל אבן, שם, ע' 92

¹¹ כך, לדוגמה, כל הנוגע לדיון ספציפי בכוחות המזוינים, ממעטת אסטרטגיית ההגנה של האיחוד האירופאי במילים. כך, קובעת האסטרטגיה שעל הכוחות המזוינים לפעול לשיפור איתנות מערכות התקשוב שלהם באמצעות שיפור יכולות הגילוי של איומים מתוחכמים במרחב הסייבר, התגובה להם והשיקום מהם. אך גם בהקשר זה, טוענת האסטרטגיה שהכוחות המזוינים אינם יכולים לפעול לבדם, אלא נדרשים לשיתוף פעולה צבאי-אזרחי ושילוב בין גישות צבאיות וגישות אזרחיות. האסטרטגיה גם קובעת שיש לבחון את תחומי האחריות של האיחוד האירופאי ושל נאט"ו בכל הנוגע לשיפור איתנות תשתיות המידע החיוניות של הממשלות, של הצבאות ושל גורמים אחרים, כדי למנוע כפילויות וכדי לשפר את ההשלמה ההדדית בין יכולות הגופים.

High Representative of the European Union for Foreign Affairs and Security Policy, **Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace**, Brussels: European Commission, Feb. 2 2013, p. 11

בדומה לאסטרטגיה של האיחוד האירופאי, גם מסמך אסטרטגיה של משרד ההגנה האמריקני – מסמך צבאי יותר מטבע מאסטרטגיית האיחוד האירופאי - קובע שהגנת מרחב הסייבר אינה משימה צבאית בלבד, אלא משימה לאומית, הכוללת שיתוף פעולה עם כלל גופי הממשל, עם המגזר הפרטי ואף עם שותפים רב-לאומיים.

The Department of Defense Cyber Strategy, Washington, DC: Department of Defense, 17 Apr. 2015, p. 7

סוגיות מרכזיות בפעולת המדינה במרחב הסייבר

מנקודת ראותה של המדינה, אפשר לסווג את הסוגיות השונות הנוגעות לפעולה במרחב הסייבר ולאבטחתו למספר תחומי אב, כדלהלן:

- סוגיית חלוקת הסמכויות בין המדינה למגזר הפרטי ותפקידו של המגזר הפרטי באבטחת מרחב הסייבר.
- חקיקה, נורמות רגולציה ותקנון.
- שיתוף מידע בין הגורמים השונים העוסקים באבטחת מרחב הסייבר.
- בניין כוח – ארגון, בניית יכולות ומחקר ופיתוח בתחום אבטחת מרחב הסייבר.
- תיאום בין הגורמים השונים הפועלים במרחב הסייבר.

להלן נעסוק בכל אחד מתחומי אב אלה.

חלוקת סמכויות בין המגזר הפרטי לממשלה

כמו כן, בשונה מהמרחבים הפיזיים שנמצאים, במידה רבה, בבעלותן המלאה או החלקית של מדינות, נמצא רוב מרחב הסייבר בבעלות פרטית (ולעיתים אף של חברות על לאומיות). לפיכך, בכל היבטי הפעולה במרחב הסייבר, נדרש לדון במקום המדינה אל מול המגזר הפרטי ובאופן בו שני המגזרים האלה פועלים ביחד.

המדינה לרוב כוללת מספר קטן יחסית של ארגונים וסוכנויות העוסקות כל אחת בתחום עיסוק מוגדר. בשל כך, לשם ההגנה על מרחב הסייבר נוטות ממשלות שונות להקים גופים שונים, או לחילופין להטיל את המשימה על גופים קיימים העוסקים בנושאים ביטחוניים או בנושאים קרובים. לדוגמה, בארה"ב, המשרד להגנת המולדת (Department of Homeland Security), שאחראי לביטחון הפנים ברמה הפדראלית, אחראי גם להגנה על כל הרשתות של כל סוכנויות הממשל הפדראלי **מלבד** אלה של קהיליית המודיעין ושל משרד ההגנה.¹² בישראל יש שורה של גורמים ממשלתיים הלוקחים חלק במלאכת ההגנה במרחב הסייבר – צה"ל, השב"כ, המוסד, המטה הקיברנטי הלאומי, הרשות הלאומית להגנה בסייבר, היחידה להגנת הסייבר בממשלה, גופים בבנק ישראל ומשרד האוצר, הרשות למשפט טכנולוגיה ומידע ומשטרת ישראל. גופים אלה – כולם או חלקם – אמורים לפעול הן במישור המעשי, הן במישור הרגולטורי והן במישור התיאום וההכוונה. כמו כן, גופים אלה – כולם או חלקם – אמורים לסייע

¹² David Clarck, Thomas Berson and Herbert S. Lin (eds.), **Op. Cit.**, Washington, DC: National Academies Press, 2014, p. 37

בהגנה הן על גופי הממשלה, הן על התשתיות החיוניות והן על גורמים שונים במגזר הפרטי, זאת בנוסף לשורה של גופים פרטיים העוסקים גם הם באבטחת מידע ובהגנה בסייבר.¹³

מנגד, המגזר הפרטי מבוזר הרבה יותר וכולל גורמים רבים העוסקים בתחומי עיסוק שונים ומגוונים. כמו כן, יש גופים רבים במגזר זה שמרחב הסייבר חיוני לפעולותיהם – אך פעמים רבות, פעולותיו של כל ארגון במרחב שונות מאלה של ארגונים אחרים. גורמים אלה נעים מעסקים קטנים המסתמכים על רכישות מקוונות ופרסום מקוון, דרך חברות היי-טק המתמחות בטכנולוגיית מידע וכלה במוסדות פיננסיים המשתמשים במרחב לשם ביצוע עסקאות ברחבי העולם. כל הגורמים הפרטיים הפועלים במרחב הסייבר עשויים להיות חשופים הן לתוקפים פליליים והן לתוקפים אחרים המנסים להשיג מטרות פוליטיות. עם זאת, המצב כיום הוא שבמרחב הסייבר, מגנים על עצמם ארגונים פרטיים באופן פרטני – הן בכל הנוגע לעיצוב הרשת הארגונית, הן בכל הנוגע לפעולה בתגובה לחדירה והן בכל הנוגע לשיקום לאחר החדירה.¹⁴ בהתאם, מידת המודעות וההשקעה במגזר הפרטי באבטחת מרחב הסייבר משתנה מארגון לארגון (וממדינה למדינה). כך, בארה"ב לדוגמה, המגזר הפיננסי לרוב מוגן היטב (יחסית) מפני תקיפות במרחב הסייבר – אפילו ביחס לחלק מהתעשייה הביטחונית – ואילו מגזרים אחרים, כגון מגזר הבריאות, לוקים בתחום זה.¹⁵ מידת ההגנה של המגזר הספציפי לא תמיד קשורה למידת החיוניות שלו למדינה. כך, בארה"ב, מידת ההגנה של מגזר האנרגיה לוקה בחסר והממשלה מתקשה לשפרה, בין השאר כיוון שתשתית זו נמצאת בידיים פרטיות ובמידה משמעותית אינה נמצאת תחת רגולציה פדרלית – למרות חשיבותה הקריטית לקיום התקין של המדינה.¹⁶

המגזר הפרטי מחזיק המחזיק בבעלות על 90% ממרחב הסייבר. לפיכך, בשונה מאשר במרחבים הפיזיים, בהם למדינה מונופול על ההגנה הלאומית, במרחב הסייבר, משמש המגזר הפרטי גם חלק במערך ההגנה המדינתי – הן כ"צרכן ישיר" של ההגנה של המדינה, הן כחלק ממערך ההגנה הנובע מעצם ההגנה של החברות על עצמן והן כחלק פעיל ממערך ההגנה הלאומית – בעיקר של חברות שעצם עיסוקן הוא הגנה במרחב הסייבר.¹⁷ בהתאם, כמות

¹³ שמואל אבן, שם, ע"מ 95-97

¹⁴ שמואל אבן, שם, ע' 93

¹⁵ P. W. Singer, "How the United States Can Win the Cyberwar of the Future", Foreign Policy, 18 Dec. 2015, www.foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/

¹⁶ Garance Burke and Jonathan Fahey, "AP Investigation: US Power Grid Vulnerable to Foreign Hacks", ABC News, 21 Dec. 2015, www.abcnews.go.com/US/wireStory/ap-investigation-us-power0grid-vulnerable-foregin-hacks-35882487

¹⁷ שמואל אבן, שם, ע' 93

משמעותית מיכולות ההגנתיות של המדינה במרחב הסייבר – הן מבחינת יכולות נטו והן מבחינת מחקר ופיתוח – עשויות להימצא בידיים פרטיות ולהגיב לשוק הפרטי יותר מאשר לגופי הביטחון.¹⁸ כיוון שרוב תשתית טכנולוגיית המידע נבנית על ידי המגזר הפרטי, מופעלת על ידו ונמצאת בבעלותו, שיפור מצב אבטחת מרחב הסייבר תחייב פעולה של הגורמים הרלוונטיים במגזר הפרטי, גם אם בסיוע של הממשלה.¹⁹

ישנה תמימות דעים בנוגע לכך שהמגזר הפרטי הוא גורם חיוני לפתרון בעיות אבטחת מרחב הסייבר. כך, לדוגמה, אסטרטגיית מרחב הסייבר של משרד ההגנה האמריקני קובעת את הקשר עם המגזר הפרטי כאחד מפעילויות משרד ההגנה לאבטחת מרחב הסייבר. אסטרטגיה זו קובעת שאבטחת מרחב הסייבר היא משימה של כל הממשל הפדרלי ושלשם השלמתה נדרש משרד ההגנה לפעול בשיתוף פעולה עם סוכנויות אחרות, שותפים בין לאומיים וחשוב מכל, עם המגזר הפרטי.²⁰ עוד מגדילה אסטרטגיה זו וקובעת שהתפקיד של ממשלת ארה"ב בהגנה על ארה"ב מפני התקפות במרחב הסייבר הוא קטן ומוגבל (בעיקר להגנה מפני התקפות סייבר בעלות השלכות משמעותיות) ואילו המגזר הפרטי הוא קו ההגנה הראשון במרחב זה. בהתאם, קובעת האסטרטגיה שממשלת ארה"ב תשקיע משאבים כדי להגן על המדינה מההתקפות המסוכנות ביותר ואילו חברות במגזר הפרטי נדרשות להשקיע בשיפור אבטחת רשתותיהן בעצמן – גם כדי לשפר את אבטחת מרחב הסייבר של ארה"ב באופן כללי.

21

אסטרטגיית אבטחת הסייבר של האיחוד האירופאי טוענת שמחד גיסא, ההתמודדות עם אתגרי אבטחת מרחב הסבר נמצאת בעיקר באחריות המדינות החברות באיחוד האירופאי (כאשר האיחוד עצמו הוא גורם המסוגל לסייע להן במאמציהן) ומאידך גיסא שהמגזר הפרטי הוא גורם מוביל באבטחת מרחב הסייבר. לדבריה, "המגזר הפרטי מחזיק בבעלות על חלקים ניכרים ממרחב הסייבר ומפעיל אותם ולפיכך כל יוזמה שמטרתה להצליח בתחום זה [להבטיח מרחב סייבר חופשי ובטוח] נדרשת להכיר בתפקיד המוביל שלו". עוד קובעת האסטרטגיה שלשם השגת איתנות במרחב הסייבר, על המדינות ועל המגזר הפרטי לשתף פעולה ולפתח יכולות למנוע תקריות במרחב הסייבר, לאתרן ולהתמודד עימן. האיחוד האירופאי, בתורו, יכול לסייע להן במאבק בסיכונים בעלי אופי חוצה גבולות ובתיאום בין השחקנים השונים בעיתות משבר. בהתאם, החקיקה של האיחוד האירופאי מטילה במקרים רבים על ספקי השירותים

¹⁸ Richard J. Danzig, **Surviving on a Diet of Poisoned Fruit – Reducing National Security Risks of America's Cyber Dependencies**, Center for a New American Security, July 2014, p. 18

¹⁹ David Clarck, Thomas Berson and Herbert S. Lin (eds.), **Op. cit.**, p. 6

²⁰ **The Department of Defense Cyber Strategy**, Washington, DC: Department of Defense, 17 Apr. 2015, p. 3-4, 7

²¹ **The Department of Defense Cyber Strategy**, p. 5

המסחריים אחריות לנטר את הרשתות ו\או המידע שבאחריותם ולדווח על תקריות ופרצות שגילו. עם זאת, אסטרטגיה זו מודה שקיימים עדיין פערים בעניין זה – בעיקר בכל הנוגע ליכולות של המדינות, לתיאום במקרים חוצי גבולות ובכל הנוגע למעורבות המגזר הפרטי ומוכנותו.²²

עם זאת, כאמור, "המגזר הפרטי" אינו מונוליטי, אלא כולל מגוון נרחב של שחקנים, בעלי יכולות וכוונות שונות בכל הנוגע למרחב הסייבר ובכלל. לדוגמה, לשחקנים שונים במגזר הפרטי שיעורי ההשקעה בכל הנוגע לאבטחת מרחב הסייבר.²⁴ לכן, בפעולה עם המגזר הפרטי, אל לממשלה להתייחס אליו כגורם אחוד. אלא עליה להתאים את תוכניות הפעולה שלה לכל תת-מגזר בתוך המגזר הפרטי (מגזר ההיי-טק, מגזר התעשייה הכבדה, מגזר השירותים, מגזר הפיננסים וכו.). כמו כן, כל תת-מגזר שכזה צריך לעבוד אל מול הסוכנויות הממשלתיות הרלוונטיות לו.²⁵

אפשר לראות שלגופים שונים במגזר הפרטי יכולות שונות בנוגע להגנה על עצמם במרחב הסייבר. סקר של חברת CWP גילה שיש מתאם ברור בין גודל החברה לבין יכולת לגלות בעמה פריצות במרחב הסייבר. לפי הסקר, בשנת 2014 הצליחו חברות גדולות²⁶ לגלות פריצות במרחב הסייבר בשיעור הגדול פי 31 מאשר חברות קטנות²⁷ ופי 2 יותר מחברות בינוניות.²⁸ כך, נראה שרוב העסקים (שאינם מתמחים באבטחת מרחב הסייבר – ועל אחת כמה וכמה העסקים הקטנים והזעירים) מתקשים לשכור את כוח האדם המתאים לשם אבטחתם. לפיכך, רוב הפרצות (81% בשנת 2014²⁹) מתגלות על ידי גורמים חיצוניים ולא על ידי החברה שפרצו למערכתיה - וזאת בשונה מאשר אירועים פליליים אחרים. בשנת 2013, רוב החברות המסחריות לא גילו את הפרצות בעצמן, אלא הפרצות התגלו על ידי צד שלישי (63% מהפרצות). מתוך הפרצות שהתגלו על ידי גורם חיצוני באותה השנה, כ-42% התגלו על ידי גורמי אכיפת החוק (גורמים מדינתיים).³⁰ בשנת 2014, גילו את הפרצות במגזר הפרטי הגורמים הבאים: גופי רגולציה\חברות אשראי\בנקים (58%), גופי אכיפת חוק (12%³¹),

²² High Representative of the European Union for Foreign Affairs and Security Policy, **Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace**, Brussels: European Commission, Feb. 2 2013, pp. 2, 4-5

²³ Jason Healey, **Breaking the Cyber-Sharing Logjam**, Atlantic Council, Feb. 2015, p. 2

²⁴ David Burg et. al., **US Cybersecurity: Progress Stalled – Key Findings from the 2015 US State of Cybercrime Survey**, PwC, July 2015, p. 5

²⁵ Richard J. Danzig, **Op. cit.**, p. 23

²⁶ משמע חברות בעלות 10,000 עובדים ויותר
²⁷ חברות בעלות פחות מ-1,000 עובדים.

²⁸ David Burg et. al., **US Cybersecurity: Progress Stalled – Key Findings from the 2015 US State of Cybercrime Survey**, PwC, July 2015, p. 3

²⁹ עליה של 10% משנת 2013

³⁰ Mandiant 2013 Threat Report - **M-Trend: Attack the Security Gap**, pp. 2-3

³¹ ביחס ל-3% בשנת 2013

לקוחות (4%) וגורמים אחרים (שאינם החברות – 7%).³² אף כי נתונים אלה חלקיים בלבד³³, אנו למדים מהם, מחד גיסא, על הפער הגדול הקיים ביכולות של רוב החברות (ושל גורמי אכיפת החוק) לגלות פרצות במרחב הסייבר, אך גם על המיומנות המשמעותית של חלק מהמגזר הפרטי בתחום (בעיקר של גורמים פיננסיים), מאידך גיסא. מגמה מעניינת נוספת היא שנראה כי כאשר ארגונים יכלו לגלות פרצות בעצמם, הם הצליחו לגלותן מהר יותר. כך, הזמן החציוני לגילוי פרצה באופן עצמאי עמד בשנת 2014 על 10 ימים (ביחס ל-31.5 בשנת 2013) ואילו לגילוי פרצה על ידי גורם חיצוני נדרשו באופן חציוני 126 ימים בשנת 2014 (ביחס ל-108 ימים בשנת 2013).³⁴ מובן שסוגיית אבטחת מרחב הסייבר אינה נוגעת לגילוי בלבד, אלא גם להכלה ולצמצום הנזק – וגם בנושא זה לכוח אדם מיומן משקל משמעותי. בהתאם, ארגונים שמסוגלים לאתר פרצות בעצמם, לרוב גם יודעים להכיל אותן בעצמם במהירות גבוהה יותר. כך, הזמן החציוני שנדרש להכלת פרצה מרגע איתורה עמד (בשנת 2014) על יום אחד בארגונים שגילו את הפרצה בעצם ועל 9 ימים בארגונים שנעזרו בגורמי חוץ (ביחס ל-14 ימים בשנת 2013).³⁵

למדינה ולמגזר הפרטי יש יתרונות שונים בכל הנוגע להגנה במרחב הסייבר. למדינה יש יתרון (לעיתים) במודיעין וביכולת לרכז את הגורמים השונים ולהשקיע משאבים ניכרים בתחום ההגנה במרחב הסייבר, ואילו למגזר הפרטי יש משאבי מחשב רבים, כלים מתקדמים וכוח אדם בעל ידע ומומחיות שאפשר לרתום לטובת הגנה על גורמים במרחב הסייבר. עם זאת, יש גם פערים מסוימים בין הצדדים. לדוגמה, מבחינת מדיניות, גורמים פרטיים מחויבים לפרטיות המשתמשים שלהם ולמוניטין שלהם, מחויבות שעשויה להקשות עליהם לשתף פעולה עם גורמי ביטחון בפרט וממשלות בכלל. כמו כן, חברות רב לאומיות עשויות להיתקל בניגוד אינטרסים בבואן לשתף פעולה עם מדינות שונות בהן הן פועלות, כיוון שלכל מדינה אינטרסים שונים ולעיתים אף מנוגדים.³⁶ כך, לדוגמה, הממשל האמריקני נוטה לתעדף תחרות ביטחונית ולהתעלם מתחרות כלכלית – הן באופן כללי והן במרחב הסייבר – בעוד שממשלת סין נוטה לתעדף תחרות כלכלית על חשבון התחרות הצבאית. בהתאם לכך, ממשלת ארה"ב נוטה להבחין בין פעולות ושחקנים ממשלתיים ופעולות ושחקנים פרטיים וממשלת סין (וממשלות אחרות) לא נוטות להבחין בין המגזר הממשלתי למגזר הפרטי. מכאן, דרך פעולה זו תקשה על

³² Trustwave Global Security Report 2015, p. 22

³³ הנתונים לקוחים מתוך דוחות של חברות אבטחת סייבר פרטיות. מכאן השונות בנתונים הספציפיים, עם זאת, על אף השונות בנתונים, ברורה המגמה.

³⁴ לפי דו"ח של חברת Trustwave, בשנת 2014, הזמן הממוצע שנדרש לזהות פריצה מרגע הפריצה עד זיהויה עמד על 188 יום ואילו הזמן החציוני עמד על 86 ימים. בכל הנוגע להכלת הבעיה – הזמן החציוני מהפריצה ועד ההכלה עמד על 111 ימים. לצורך הכלה נדרשו (באופן חציוני) 7 ימים בלבד. רוב הפרצות (85%) התגלו לפני סיום השימוש בפרצה. ראה:

Ibid, p. 23-25

³⁵ Ibid, p. 26

³⁶ שמואל אבן, שם, ע' 98

הממשל האמריקני להגן על האינטרסים הכלכליים שלו במרחב הסייבר ולשלב בין שיקולים כלכליים וביטחוניים בפעולה במרחב זה, בין השאר מכיוון שהאינטרסים הכלכליים מוחזקים במידה רבה על ידי חברות פרטיות, בעוד שהממשל הסיני עשוי לפעול במרחב הסייבר גם בסיוע לגורמים הנחשבים "פרטיים" (לדוגמה, על ידי ריגול תעשייתי באופן ישיר או עקיף).³⁷ לכן שיתוף הפעולה של גורמים במגזר הפרטי עם המדינה אינו תמיד פשוט, גם כאשר ברור לכל שהוא הכרחי.³⁸ מכאן, בהינתן פערי היכולות הקיימים במגזר הפרטי ופערי המדיניות בכל הנוגע לאבטחת מרחב הסייבר, נשאלת השאלה מה תפקיד המדינה באבטחת המגזר הפרטי? גישה אחת טוענת שלמדינה יש אינטרס מיוחד במעורבות בהגנת מרחב הסייבר של המגזר הפרטי כאשר קיים סיכון לאירוע בעל השפעה מערכתית שלילית על המדינה או כאשר קיים סיכון להתקפה מצד אויב. לפי גישה זו, סדר העדיפויות להתערבות הממשלה יקבע לפי הערכת תוחלת הנזק,³⁹ גורם הסיכון ועלות הפחתת הנזק (במונחי זמן וכסף) ביחס לתוחלת הנזק.⁴⁰ כך לדוגמה, בארה"ב רוב התשתיות החיוניות נמצאות בידיים פרטיות. כיוון שתוחלת הנזק של פגיעה בתשתיות אלה היא גבוהה, סיכון הפגיעה בה גבוה ועלות השיקום גבוהה, יש הטוענים שנדרשת רגולציה משמעותית יותר על גורמי התשתיות החיוניות בכל הנוגע לביטחון סייבר.⁴¹ בדומה לכך, האסטרטגיה של האיחוד האירופאי קובעת שהתגובה של האיחוד האירופאי לתקרית או להתקפה במרחב הסייבר תשתנה לפי אופי האירוע, היקפו והשלכותיו, כדלהלן:⁴²

- במקרה שלאירוע השלכות משמעותיות על המשכיות הפעולה העסקית, יופעלו תוכניות שיתוף הפעולה של גורמי אבטחת הרשתות ומערכות המידע ברמה הלאומית או ברמת האיחוד – בהתאם להיקף האירוע. גופים אלה יחלקו במידע ויסייעו האחד לשני.
- במידה והאירוע פלילי באופיו, סוכנות יורופול ו\או המרכז האירופאי לפשיעה במרחב הסייבר (European Cybercrime Center – EC3) יידעו ויפעלו בשיתוף עם גורמי אכיפת חוק מדינתיים מהמדינות שהושפעו.
- במידה והאירוע הוא ביטחוני באופיו (ריגול או התקפה על ידי גורם מדינתי) או שהשלכותיו נוגעות בביטחון הלאומי, יתריעו גורמי הביטחון הלאומי בפני מקביליהם הרלוונטיים שהם נתונים בהתקפה כך שיוכלו להגן על עצמם. בשלב זה יופעלו מנגנוני

³⁷ Richard J. Danzig, *Op. cit.*, pp. 22-23

³⁸ שמואל אבן, שם, ע' 98

³⁹ מכפלת אומדן הנזק והערכת הסבירות לפגיעה.

⁴⁰ שמואל אבן, שם, ע' 102

⁴¹ Martin C. Libicki, "Don't Buy the Cyberhype", *Foreign Affairs*, Aug. 14, 2013, www.foreginaffairs.com/articles/united-states/2013-08-14/dont-buy-cyberhype

⁴² High Representative of the European Union for Foreign Affairs and Security Policy, *Op. cit.*, pp. 18-19

ההתרעה המוקדמת ובמקרה הצורך גם גורמים אחרים (ניהול משברים וכו). אפשר שהתקפה בעלת השלכות רציניות מספיק תוכל להיות עילה להפעלת סעיף הסולידריות הלאומית (סעיף 222).

- במידה והאירוע פגע במידע אישי, יפעלו גורמי אבטחת המידע האישי.

גישה נוספת היא שחלוקת האחריות בין המדינה למגזר הפרטי תתבסס על גודל האיום וחומרתו. לפי גישה זו, תבחין המדינה בין האיומים על סמך מידת התחכום שלהם ותערוך הפרדה בין הגנה כנגד איומים מתוחכמים ובין הגנה נגד איומים לא מתוחכמים. כך, הגנה נגד איומים לא מתוחכמים (חובבים, פעילי-סייבר, פושעים וכו) תתבצע על ידי הגופים המותקפים עצמם וגופי אכיפת חוק מדינתיים ומנגד, הגנה כנגד איומים מתוחכמים (לדוגמה שחקנים מדינתיים) תצריך את תשומת הלב של ארגוני הביטחון הלאומי למיניהם. חלוקה זו מתבקשת הן עקב הנזק שאיומים מתוחכמים יכולים לגרום, הן עקב המטרות שלהם (שלעיתים קרובות נוגעות לכשעצמן בביטחון הלאומי) והן עקב מורכבות האיום והיכולות שברשות הגורמים העומדים מאחוריו.⁴³

אפשר גם שהמדינה תסייע למגזר הפרטי בראש ובראשונה בתפקידה המסורתי כאוכפת החוק והמענישה. כך, לדוגמה, במקרה של הפריצה למחשבי סוני בשנת 2014, הציעה ממשלת ארה"ב לסוני סיוע, בעוד שהבולשת הפדרלית (FBI) חקרה את האירוע – כמו כל אירוע פלילי אחר – מתוך כוונה להעמיד את המבצעים לדין פלילי. עם זאת, אפשר שבחקירה פלילית רגילה והעמדה לדין של התוקף לא יהיה כל סיוע לגורם המותקף, כיוון שחקירה פלילית אינה חקירה מקצועית ומניעתית, אלא מטרתה מציאת אשמים והענשתם. כך, לדוגמה, בסיוע של ארה"ב לסוני בשנת 2014 והחקירה הפלילית שנוהלה באותה עת, שאלת זהות התוקף עמדה במרכז הדיון והושפעה, בחלקה, משיקולים פוליטיים.⁴⁴ עבור ארה"ב היה ערך רב במציאת מקור ההתקפה, אך עבור סוני עצמה, לא הייתה משמעות מיוחדת לידיעה שלאחר מעשה האם התוקף הגיע מצפון קוריאה, סין או רוסיה.

חשיבות מיוחדת ניתנת לשאלת ההגנה הפעילה⁴⁵ על המגזר הפרטי ועל ידי גורמים במגזר זה. בעוד שאין חולק על כך שהארגונים השונים צריכים לנהל את ההגנה הסבילה על רשתותיהם, נשאלת השאלה מי היא הסוכנות שתנהל את ההגנה הפעילה על הרשתות השונות – הן הממשלתיות, הן הצבאיות, הן החיוניות והן האזרחיות "האחרות" – ובייחוד את החלקים

⁴³ Richard J. Danzig, *Op. cit.*, p. 29

⁴⁴ Adam Segal, "America is Learning the Hard Way How To Respond to Cyber Threats", *Defense One*, 18 Dec. 2014

⁴⁵ הגנה פעילה פירושה יכולת גילוי איומים, איתורם וצמצומם בזמן אמת. בין השאר מדובר בהונאה בסייבר, בשיבוש מונע של רשתות יריבות ובתקיפות מקדימות בסייבר. לדיון בהגנה פעילה ראה: David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, p. 48-50

ההתקפיים יותר של ההגנה הפעילה. לכאורה אפשר לטעון שבדומה ל"מרחבים הפיזיים", גם במרחב הסייבר תתחלק האחריות ל"הגנה הפעילה" בין הצבא לבין סוכנויות הביטחון השונות (פנים וחוץ)⁴⁶. עם זאת, בהינתן היתרונות של ההגנה המניעתית (פרו-אקטיבית) ויכולות הסייבר הניכרות הנמצאות בידיהם של חלק מגורמי המגזר הפרטי, נשאלת השאלה האם יוכל המגזר הפרטי (באופן חוקי או בלתי חוקי) לערוך "תקיפות מנע" במרחב הסייבר ואם כן, כנגד אילו שחקנים ובאילו הקשרים? אם התשובה היא שלילית, יש לדון בסוגיית אכיפת האיסור על תאגידי-על רב-לאומיים ולשאול, בין השאר האם (וכיצד) יכולה מדינה בכלל לאכוף דבר מה על תאגיד רב לאומי כגון גוגל, המחזיק בידו בעלות על חלקים ניכרים מתשתית האינטרנט. סוגיית ההגנה הפעילה, שהיא פועל יוצא מהחזקת יכולות סייבר בידיים פרטיות מחייבת דיון בשאלת הבסיס האם יש למדינה מונופול על האלימות במרחב הסייבר? ואם כן (ואם לא) היכן גבולות הסמכות של המדינה במרחב זה?⁴⁷

חקיקה, נורמות, רגולציה ותקנון

כיוון שמרחב הסבר הוא מרחב חדש, ניכרים כיום מגוון פערים בכל הנוגע להסדרת הפעולה בו מבחינה חוקית – אפילו ברמות בסיסיות מאוד.

כך לדוגמה, בארה"ב קיים פער אפשרי בכל הנוגע לתקיפה על ידי המדינה במרחב הסייבר, כיוון שחוק סמכויות המלחמה (War Powers Act – 1973) והחוקה אינם מכסים כראוי את סוגיית הפעלת הכוח הצבאי במרחב הסייבר. הגבלות אלה מתחדדות כאשר הן מתווספות להגבלות הקיימות על הפעלת הכוחות המזוינים האמריקניים בתוך ארה"ב באופן כללי (לדוגמה מכוח Posse Comitatus Act – 1878), אפילו תוך כדי שיתוף פעולה עם סוכנויות אזרחיות או בסיוע להן. מכאן, עולות שאלות בדבר היכולת להפעיל את הכוחות המזוינים האמריקניים כנגד התקפות סייבר על ארה"ב מתוך ארה"ב, או על מטרות עוינות בתוך ארה"ב. נוסף על כך, ישנו פער בדין הבין לאומי בכל הנוגע לפעולות עוינות במרחב הסייבר – הן פליליות והן מדינתיות - החוצות גבולות לאומיים. במיוחד ניכר הפער בכל הנוגע לתחולת דיני המלחמה על מרחב הסייבר. קיימים גם פערים בין החוקים השונים של המדינות השונות שעוסקים במרחב הסייבר. כל הפערים הללו עשויים להקשות על הפעולה נגד איומים במרחב הסייבר או אף למנוע אותה כליל ולכן נדרשתל הסדרה מקיפה בכל הנוגע לחוקים, לתקנות ולדינים השונים הנוגעים לפעולה במרחב הסייבר.⁴⁸

⁴⁶ כבר כיום עורכות ממשלות פעילויות "הגנה פעילה" שמשלבות הן סוכנויות אכיפת חוק והן גורמים במגזר הפרטי – כמו הפעולה של הממשל האמריקני (באמצעות הבולשת הפדרלי) במאי 2013 נגד מפעיל Botnet סיטל (Citadel) שנערכה בסיוע חברת מייקרוסופט ובחסות צו בית משפט.

⁴⁷ David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, p. 48-55, 77

⁴⁸ *Ibid*, pp. 56-58

המדינה היא הבורר הסופי בשטחה בכל הנוגע למותר ולאסור. על אף שמרחב הסייבר הוא מרחב "על מדינתי", הציוד, התשתיות והאנשים המשמשים לקיומו נמצאים במרחבים הפיזיים, הנשלטים על ידי מדינות. לפיכך, למדינה מקום משמעותי בכל הנוגע לקביעה של מה מותר לעשות במרחב הסייבר, מה אסור לעשות בו וכיצד יש לפעול במרחב זה. בהתאם, האסטרטגיה של האיחוד האירופאי טוענת, לדוגמה, שהמענה לאתגרים השונים בתחום הפשיעה במרחב הסייבר נמצא בשיפור החקיקה, שיפור היכולות של גופי אכיפת החוק ושיפור התיאום בין גופי האכיפה, גופי המשפט, המגזר הציבורי והמגזר הפרטי (הן באירופה והן מחוצה לה).⁴⁹

בראש ובראשונה, נדרשת המדינה לקבוע אילו פעולות (עוינות) במרחב הסייבר נחשבות לפעולה פלילית (כגון גניבה או ריגול כלכלי) ואלו נחשבות כפעולה ביטחונית (כגון ריגול ביטחוני). כמו כן, עליה לקבוע איזו פעולה עוינת היא תוקפנית ואיזו אינה (ומה מדיניות התגובה לפעולות השונות). כך לדוגמה, נשאלת השאלה האם ריגול במרחב הסייבר הוא פעולה תוקפנית, או שמא פעולה עוינת שאינה תוקפנית? יש מדינות שעשו הסדרה כללית כל שהיא בעניינים אלה. לדוגמה, אפשר באופן כללי להגיד שבארה"ב, אם היקף האירוע במרחב הסייבר מצומצם, אם הנכס הנתקף אינו ביטחוני או שאינו תשתית חיונית ואם הנזק אינו משמעותי, יתויג האירוע כפלילי. מנגד, אירוע שנזקו משמעותי (או פיזי) יחשב כמעט תמיד כאירוע ביטחוני. גורמים נוספים שעשויים להשפיע על קטלוג האירוע הוא מקור ההתקפה (מבחינה גיאוגרפית) וזהות התוקף.⁵⁰

חלק מרכזי אחר מההסדרה שמבצעת המדינה במרחב הסייבר הוא ההסדרה של פעולותיה ושל סמכויותיה במרחב. פעולות שונות, כנגד גורמים שונים ואשר להן תוצאים שונים, המתבטאים במרחבים שונים, יצריכו סמכויות אישור שונות. אין דין פעולה התקפית בעלת תוצאים פיזיים כנגד אויב כדין פעולת ריגול כנגד יריב (או ידיד) המתבצעת בשרתים שנמצאים בשטחה של מדינה שלישית. לכן, בראש ובראשונה נדרשת המדינה לקבוע באופן ברור מה הן הסמכויות השונות הנדרשות לאישור פעולות שונות במרחב הסייבר.

אם נפנה לבחון את הנעשה בפועל, נגלה שכבר כיום, יש חוקים רבים העוסקים באבטחת מרחב הסייבר. בארה"ב, לדוגמה, היו (נכון לשנת 2013) מעל 50 חוקים פדרליים (חלק בני

⁴⁹ High Representative of the European Union for Foreign Affairs and Security Policy, **Op. cit.**, p. 10

⁵⁰ David Clarck, Thomas Berson and Herbert S. Lin (eds.), **Op. cit.**, p. 58

קרוב לשלושים שנה⁵¹ ואף יותר⁵² שעסקו באופן זה או אחר באבטחה במרחב הסייבר ובסמכויות הגופים השונים במרחב זה. כך, נקבע כדלהלן:⁵³

- מכון התקנים הלאומי (National Institute of Standards and Technology) אחראי לפיתוח תקני אבטחה, הנחיות ושיטות רלוונטיות עבור מערכות המחשב הפדרליות שאינן שייכות למערכת הביטחון (מכוח חוק Computer Security Act -1987 וחוק תוכניות מחקר שונות בתחום אבטחת מרחב הסייבר (מכוח חוק Cyber Security Act -2002 Federal Information Security Management Act) ומוסמך לממן ולערך תוכניות מחקר שונות בתחום אבטחת מרחב הסייבר (מכוח חוק Research and Development Act -2002).
- משרד הניהול והתקציבים בבית הלבן (Office of Management and Budget) אחראי לפיתוח מדיניות אבטחת מרחב הסייבר (מכוח חוק Paperwork Reduction Act -1995), לפיקוח ולדיווח על יישום מדיניות האבטחה במרחב הסייבר של הסוכנויות השונות (מכוח חוק Federal Information Security Management Act -2002).
- ראשי הסוכנויות השונות אחראים להבטיח את איכות המדיניות והתהליכים הנוגעים לאבטחת מרחב הסייבר של הסוכנות שבראשה הם עומדים (מכוח חוק Clinger-Cohen -1996).
- המשרד לביטחון המולדת (Department of Homeland Security) אחראי לאבטחת מרחב הסייבר בהקשרי ביטחון הפנים ותשתיות חיוניות (מכוח חוק Homeland Security Act -2002).
- כל סוכנות פדרלית אחראית לאבטח בעצמה את מערכות המידע המסייעות לפעילותה ולנכסיה (כולל אלה שמנהלות על ידי קבלנים, סוכנויות אחרות או כל מקור חיצוני) ואת המידע שעליהן (מכוח חוק Federal Information Security Management Act -2002).
- כל סוכנות פדרלית נדרשת ליידע את ה-CERT הפדרלי (שהוקם מכוח חוק Federal Information Security Management Act -2002) ולהתייעץ עימו בנוגע לתקריות הקשורות לביטחון מידע וביטחון מערכות המידע המסייעים למבצעי הסוכנות או לנכסיה (כולל אלה שמנהלות על ידי קבלנים, סוכנויות אחרות או כל מקור חיצוני).

⁵¹ כדוגמת (Computer Fraud and Abuse Act (1986

⁵² כדוגמת (Federal Wiretap Act (1968 ו-(Foreign Intelligence Surveillance Act (1978

⁵³ David Clarck, Thomas Berson and Herbert S. Lin (eds.), **At the Nexus of Cybersecurity and Public Policy – Some Basic Concepts and Issues**, Washington, DC: National Academies Press, 2014, p. 55-56, 76

⁵⁴ חוק זה גם מסמיך את המוסד הלאומי למדעים (National Science Foundation) לממן מחקרים ותוכניות הנוגעים לאבטחה במרחב הסייבר.

ההסדרה החוקית משמעותית במיוחד בכל הנוגע לפעולות שנעשות נגד אינטרסים מדינתיים במגזר הפרטי – כמו לדוגמה חברות העוסקות (גם באופן עקיף) בייצור ביטחוני או תאגידים גדולים וחשובים במשק. אפשר שבהקשרים אלה תהיה המדיניות שונה בהגנה ובהתקפה.⁵⁵ בארה"ב ישנה הבחנה בין תגובה לאירוע סייבר פלילי לבין תגובה לאירוע סייבר ביטחוני. ההבחנה הברורה הזו חשובה מכמה סיבות:

- ראשית, בארה"ב, כוחות הביטחון, קהיליית המודיעין וכוחות אכיפת החוק פועלים מכוח פרקים שונים בחוק האמריקני ולפיכך נדרשת הבחנה בין אירועים שונים כדי לדעת אילו גורמים להפעיל וכיצד.⁵⁶
- שנית, התגובה לאירוע סייבר ביטחוני קלה יותר מאשר התגובה לאירוע סייבר פלילי, כיוון שהיא מסירה סייגים רבים המוטלים על פעולת גורמי אכיפת החוק.

כך, בתיאוריה, שני אירועים זהים עשויים להיות מטופלים אחרת בהתאם לסיווגם כביטחוניים או כפליליים. עם זאת, למרות השאיפה התיאורטית לבהירות, לא תמיד ברור בתחילת האירוע (ולעיתים אף בכלל) מה אופיו ומה זהות המבצע. כמו כן, המגמה היום של "איומי כלאיים" (היברידיים) עשויה להביא לכך שאיום מסוים יהיה בו זמנית הן פלילי והן ביטחוני.⁵⁷

אך לא די בהחלטה בלבד בנוגע לסוגיות אלה. כדי שהכל ידעו מה מותר ומה אסור, על המדינה לפרסם את החלטותיה העקרוניות בנוגע להסדרה החוקית והתפיסתית במרחב הסייבר. כיוון שהקו המפריד בין הפרטי לציבורי במרחב הסייבר מטושטש ומכיוון שמערכות חיוניות רבות נמצאות בבעלות אזרחית חלקית או מלאה, על המדינה להבהיר אילו מערכות פרטיות הן מערכות חיוניות וכמו כן להבהיר מה ההשלכות של חיוניותן להתערבות המדינה בהגנה עליהן. לדוגמה, יכולה המדינה להחליט שאמות המידה שנקבעו להגנה על מערכות ממשלתיות חלות גם על מערכות אלה.⁵⁸

המדינה לא רק קובעת את המותר והאסור, אלא היא גם הגוף המסדיר, במידה מסוימת, את האופן בו דברים מתנהלים במדינה במגוון תחומים – החל מקביעת שעון הקיץ וכלה בהסדרת התנועה בכבישים. לפיכך, המדינה יכולה לקבוע גם תקנים מחייבים בתחום מרחב הסייבר ובמיוחד בכל הנוגע לאבטחת מרחב זה. בהקשר זה יש הטוענים שבארה"ב, המידע והמדיניות הקיימים לא היו מספיקים, עד כה, להניע את הגורמים השונים לפעולה במטרה לשפר את ביטחונה של ארה"ב בסייבר באופן כללי – אף כי ארגונים מסוימים עשו לטובת שיפור

⁵⁵ *Ibid*, p. 72

⁵⁶ כוחות הביטחון מכוח פרק 10 (Title 10), גורמי אכיפת החוק מכוח פרק 18 (Title 18) וקהיליית המודיעין מכוח פרק 50 (Title 50).

⁵⁷ David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, p. 58

⁵⁸ Richard J. Danzig, *Op. cit.*, p. 22

אבטחתם שלהם במרחב הסייבר. זאת מכיוון שמבנה התמריצים הקיים כיום מתעדף השקעה קצרת טווח בשיפור מצב הארגון ולא השקעה בשיפור אבטחת "המערכת" (האמריקנית) בכללותה. לפיכך, יש הטוענים שנדרש לשנות מערך תמריצים זה.⁵⁹ המדינה יכולה גם להתערב במלאכת התכנון באופן פחות ישיר ולעודד או להכווין פיתוח תקנים וולונטריים על ידי התעשיות הרלוונטיות.⁶⁰ לדוגמה, האסטרטגיה של האיחוד האירופאי טוענת שהאיחוד נדרש להציב אמות מידה אחידות לאבטחה שיוטמעו בכל הגורמים העוסקים בטכנולוגיית המידע (מפתחי חומרה, מפתחי תוכנה, ספקי שירותים וכו') כך שכל טכנולוגיית המידע בה יעשה שימוש באירופה תעמוד בדרישות סף מסוימות, שיהיו אחידות לכל מדינות האיחוד. לשם כך, קובעת האסטרטגיה שיש לתמרץ בהתאם את המגזר הפרטי בדרכים שונות (כגון חובת סימון מידת אבטחה על המוצרים), כולל תמרוץ, הכוונה ותיאום של מאמצי מחקר ופיתוח רלוונטיים (גם במגזר הפרטי). עוד מדגישה האסטרטגיה את הצורך לפתח אמות מידה וולונטריות לאבטחת מחשוב הענן, תוך התמקדות במערכות השליטה התעשייתיות (Industrial Control Systems) ובתשתיות התחבורה והאנרגיה.⁶¹ בדומה לכך, אסטרטגיית משרד ההגנה האמריקני למרחב הסייבר קובעת שנדרש שינוי במרכזי הממשל הפדרלי כך שהמכרזים יטמיעו באופן מלא יותר את סוגיית הגנת המידע בתוך המערכות הנרכשות. בין המאמצים השונים בעניין זה, אפשר לכלול חיוב החברות הזוכות לחשוף פרטים על גניבת מידע באמצעות מרחב הסייבר, הטמעת תקנים רלוונטיים בתוך דרישות המכרז (ושיפור התקנים הקיימים), הרחבת תוכניות הכשרה וחינוך לביטחון במרחב הסייבר לחברות קבלניות שעובדות עבור משרד ההגנה, בחינת נהלי הסיווג בכל הנוגע למידע הנמצא על רשתות של קבלנים חיצוניים ועוד.⁶² יישום בפועל של התערבות רגולטורית של המדינה אפשר לראות בכלי הערכת אבטחת מרחב הסייבר שפיתח ה-FFIEC.⁶³ כלי זה הוא פרוטוקול שמטרתו לאפשר למוסדות הפיננסיים להעריך את אבטחת הסייבר שלהם ולנהל את סיכוניהם בתחום. דוגמה נוספת הוא הסקר שערך אגף השירותים הפיננסיים של מדינת ניו-יורק (New York Department of Financial Services) בנוגע לאבטחת הסייבר של 40 בנקים בהקשרי כשלים כתוצאה מפגיעות של גורמי צד שלישי.⁶⁴

⁵⁹ David Clarck, Thomas Berson and Herbert S. Lin (eds.), **Op. cit.**, p. 2

⁶⁰ P. W. Singer, **Op. cit.**

⁶¹ High Representative of the European Union for Foreign Affairs and Security Policy, **Op. cit.**, p. 12-13

⁶² **The Department of Defense Cyber Strategy**, Washington, DC: Department of Defense, 17 Apr. 2015, p. 23

⁶³ Federal Financial Institution Examination Council. זה הוא גוף רגולטורי של הממשל הפדרלי האמריקני שתפקידו לקבוע סטנדרטים עבור המערכת הפיננסית בארה"ב.

⁶⁴ David Burg et. al., **Op. Cit.**, p. 11

מלאכת ההסדרה לה נדרשת המדינה אינה קלה כלל ועיקר. זאת משום ששיפור האבטחה במרחב הסייבר מתנגש, פעמים רבות, עם קווי מדיניות אחרים ומגמות אחרות בחברה במגוון תחומים (בהיבטי כלכלה, חדשנות, זכויות אזרח וכו'). מסיבה זו, סוגיית ההסדרה מוטלת, ברמה העקרונית, ישירות לפתחם של מקבלי ההחלטות. לפיכך, עקב חשיבותן של מערכות הפועלות במרחב הסייבר, על מקבלי ההחלטות בעצמם לתעדף ולקבוע את עקרונות הפעולה של המדינה במרחב הסייבר ולא לאצול את הסמכויות לאנשי הטכנולוגיה או התקציבים. לפיכך, יש הטוענים שמקבלי ההחלטות נדרשים להבנה בסיסית הן של עולם "המבצעים" והן של עולם הטכנולוגיה במרחב הסייבר, כדי שיוכלו להחליט באופן נכון וענייני בנושאים החדשים והבלתי מוכרים הקשורים במרחב הסייבר.⁶⁵

כאשר המדינה וסוכנותיה נדרשות לתת מענה לבעיית אבטחת מרחב הסייבר, עליהן לתת את הדעת למגמות המנוגדות הקיימות בחברה ולנסות לפעול בהתאם. אפשר פעולת המדינה תהיה בעיקרה פעילות "עקיפה" ולא "ישירה" ותבטא, לדוגמה בצמצום חסמים בירוקרטיים, טיפול בגורמים מעכבים, תמרוץ (הן חיובי והן שלילי), תעדוף וכו'. כך, אסטרטגיית אבטחת מרחב הסייבר של האיחוד האירופאי מזהה שכיום, אין תמריצים מספיקים למגזר הפרטי לספק לממשלה נתונים אמין בכל הנוגע להתרחשות תקריות במרחב הסייבר או למידת השלכותיהן, לאימוץ תרבות ניהול סיכונים במרחב הסייבר או להשקיע בפתרונות אבטחה. לפיכך, טוענת האסטרטגיה, נדרשת חקיקה שתבטיח שהשחקנים בתחומי מפתח מסוימים (בעיקר אנרגיה, תחבורה, בנקאות, פיננסים, מוסדות ציבוריים ספקי שירות מסוימים) יעריכו את הסיכונים הקיימים להם במרחב הסייבר, יבטיחו (באמצעות ניהול סיכונים) את אמינות מערכות המידע והרשתות ואת איתנותן ויחלקו את המידע הנוצר מניהול הסיכונים שלהן עם הסוכנויות הלאומיות לאבטחת המידע והרשתות. לפי האסטרטגיה, סוכנויות לאומיות אלה יקבלו דיווח על כל תקרית בעלת השלכות משמעותיות על המשכיות שירותי הליבה והספקת הטובין המתבססים על מערכות המידע והרשתות. על סוכנויות אלה לדווח על מקרים פליליים לגורמי אכיפת החוק, לפרסם באופן גלוי וסדיר מידע בלתי מסווג בנוגע להתראות מוקדמות על תקריות וסיכונים ולתגובות מתואמות.⁶⁶

חוץ מאשר השפעה של המדינה (לדוגמה, על ידי חקיקה, הטבות מס, הקמת גופי ביצוע וכו'), חלק מהתמרוץ לשיפור האבטחה במרחב הסייבר יכול להגיע מהשוק הפרטי באופן עצמאי – לדוגמה, כתוצאה מעמידה בתנאי ביטוח מפני נזק דרך מרחב הסייבר. בהתאם, לדוגמה,

⁶⁵ Richard J. Danzig, *Op. cit.*, p. 21

⁶⁶ High Representative of the European Union for Foreign Affairs and Security Policy, *Op. cit.*, p. 6

המדינה עשויה לשפר נושאים כגון שיתוף מידע בין גורמים פרטיים לבין עצמם ובינם לבין המדינה אם תגן על גורמים אלה מתביעות – כפי שחוק CISA מנסה לעשות כעת בארה"ב.⁶⁷

עם זאת, יש להקפיד שתהליכי ההסדרה של המדינה והתקנות שיתוקנו בעקבותיהם לא יפגעו יותר מידי בגורמים חשובים אחרים כגון חדשנות (כולל מהירות הפיתוח ומחיר המוצרים) או זכויות האזרח (כולל פרטיות וההליך התקין וכו').⁶⁸ אין להתעלם מכך שתעשיית טכנולוגיית המידע היא תעשייה גלובלית המציבה את מהירות המחקר והפיתוח בעדיפות על פני גורמים אחרים. לכן, על המדינה להימנע מקביעת תקנים וחוקים שהתעשייה לא תרצה לעמוד בהם או לא תוכל לעמוד בהם, שיעכבו יתר על המידה את תהליך המחקר והפיתוח (או שייקרו אותו), או שיהיו ייחודיים למדינה עצמה ולא חלק מתקן בין לאומי הנמצא בשימוש נרחב (או אף מנוגדים לתקן שכזה). בדומה לכך, אסטרטגיית אבטחת מרחב הסייבר של האיחוד האירופאי טוענת שעל המחויבויות המשפטיות והחוקיות להשלים שיתופי פעולה וולונטריים ולא רשמיים לשיפור האבטחה ולחילופי מידע – כולל בין גופים ציבוריים ופרטיים - ולא למנוע אותם.⁶⁹

יש גם להכיר בכך שחלק מההסדרות והאינטרסים הנדרשים לשיפור האבטחה במרחב הסייבר מתנגשים עם קווי מדיניות אחרים, אינטרסים אחרים או אף ערכים מנוגדים (לדוגמה בכל הנוגע לפרטיות או לניטרליות רשת) של המדינה או של גורמים אחרים.⁷⁰ כך, לדוגמה, מומחים טוענים ששיתוף המידע בנושאי הגנת מרחב הסייבר קורה ממילא וכי יעילות ההגנות המוקנות בחוק CISA אינה רבה, ומנגד, מציב החוק סכנות משמעותיות בפני השמירה על פרטיות האזרח.⁷¹ בתוך כך, יש לזכור שלגורמים שונים – משתמשי קצה, מפתחי חומרה, ספקי שירותים, ממשלות וכו' - ישנם תמריצים שונים בכל הנוגע לאבטחה במרחב הסייבר. תמריצים אלה לא תמיד מעמידים את אבטחת מרחב הסייבר במקום הראשון בסדרי העדיפויות או לחילופין, לא תמיד מעמידים את האבטחה "הנכונה" מבחינה כללית\ציבורית על פני זו הנכונה מבחינה פרטית\ארגונית. בכך, אבטחת מרחב הסייבר דומה מאוד למשאב ציבורי (Public Good) בכך שחלק גדול מהתשואות המתקבלות מאבטחת מרחב הסייבר מועילות לחברה כולה ולא בהכרח לגורם המשקיע האינדיבידואלי. לפיכך, ישנו ויכוח בנוגע לשאלה האם אבטחת מרחב סייבר הנהוגה כיום, שהיא תוצאה של סך כל ההחלטות האינדיבידואליות של השחקנים השונים הפועלים במרחב, היא דבר שנכון לעשותו (הן מבחינה טכנית והן מבחינה

⁶⁷ Elias Groll, "Controversial Cybersecurity Measures Set for Final Approval", *Foreign Policy*, Dec. 16 2015, www.foreignpolicy.com/2015/12/16/controversial-cybersecurity-measure-set-for-final-approval

⁶⁸ David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, p. 63-64

⁶⁹ High Representative of the European Union for Foreign Affairs and Security Policy, *Op. cit.*, p. 6

⁷⁰ *Ibid*, 2-3

⁷¹ Elias Groll, *Op. cit.*

ערכית) ומה היא תפקידה של הממשלה (אם בכלל) בהכוונת אבטחת מרחב הסייבר של השחקנים האחרים בזירה ובתמרוץ ההתנהגות "הנכונה".⁷²

תחום אחר הנמצא באופן כמעט מוחלט בסמכותה של המדינה הוא גיבוש נהלי הדין הבין לאומי בכל הנוגע להתנהלות המדינה והגורמים הפועלים בשטחה ומשטחה במרחב הסייבר.⁷³ כיוון שיש פער בהתאמת הדין הבין לאומי הקיים למרחב הסייבר, המדינה נדרשת לקדם גיבוש של נורמות בין לאומיות בנוגע לשימוש במרחב הסייבר למגוון מטרות – כולל לצורך פעילות צבאית התקפית ופעילות ריגול. נורמות אלה יכולות להיקבע הן במסגרת רשמית של אמנות והסכמים (דו-צדדיים או רב-צדדיים, כגון Convention on Cybercrime⁷⁴) והן במסגרת פחות רשמית או מחייבת כגון ניירות עמדה, הכרזות של מקבלי ההחלטות ופעולות בשטח. בדומה לנורמות בינ"ל אחרות, כך גם כל נורמה במרחב הסייבר תהיה גורם מכווין ומקור לגיטימציה ולא תמנע, לכשעצמה, פעולות אסורות במרחב ודרכו. אף על פי כן, אפשר שנורמות אלה תוכלנה, אולי, למנוע את הסף העליון והמסוכן ביותר של פעולות במרחב הסייבר (לדוגמה – השבתה נרחבת על תשתיות אזוריות).⁷⁵ בהתאם, הכריזו מדינות שונות על דרכי פעולתן במרחב הסייבר. כך, הכריזה ארה"ב שדיני המלחמה חלים במרחב הסייבר ושכל הנוגע למבצעים במרחב הסייבר, היא תנהג בהתאם לדיני המלחמה הנהוגים כיום במרחבים הפיזיים.⁷⁶ האסטרטגיה של האיחוד האירופאי קובעת שבזירה הבין לאומית, ישאף האיחוד האירופאי לקדם פתיחות וחופש באינטרנט, לעודד מאמצי פיתוח נורמות התנהגות וליישם את הדין הבין לאומי הקיים במרחב הסייבר. עוד קובעת האסטרטגיה שהאיחוד האירופאי יפעל אל מול מדינות שאינן חברות באיחוד כדי להשיג רמה גבוהה של שמירה על נתונים – כולל נתונים אישיים, יפעל לקידום מרחב הסייבר כמרחב של חירות ושל זכויות בסיסיות, יקדם אחריות חברתית של התאגידים ויפעל לשיפור התיאום הבין לאומי בנושא, יקדם מאמצים להגדרת נורמות התנהגות במרחב הסייבר שכל השחקנים בו יוכלו לפעול על פיהם ויפעל לקידום בניית אמון ושקיפות בכל הנוגע לאבטחת מרחב הסייבר כדי לצמצם את הסיכון מהבנה לא נכונה של פעולת מדינה זו או אחרת במרחב. בהמשך, קבע האיחוד שהוא אינו קורא ליצירת מכשירים חוקיים חדשים למרחב הסייבר ותומך ביישום המכשירים, החוקים והאמנות הקיימים – כולל הדין ההומניטארי הבינ"ל במקרה של עימותים במרחב הסייבר. לבסוף קובעת האסטרטגיה שהאחריות למרחב סייבר בטוח יותר מוטלת על כל השחקנים בסביבת המידע הגלובלית –

⁷² David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, pp. 2-3, 52

⁷³ *Ibid*, p. 76

⁷⁴ *Ibid*, pp. 57-58

⁷⁵ P. W. Singer, *Op. cit.*

⁷⁶ David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, p. 76

החל מהאזרח וכלה בממשלה. הן האזרחים והן הממשלות צריכים לפעול על פי הנורמות והחוקים הנהוגים במרחב הסייבר – כמו במרחב הפיזי.⁷⁷

ניתן להניח שמאמצי ההסדרה השונים שתערוך המדינה יחייבו תעדוף, פשרות וקבלת החלטות על ידי הגורמים המתאימים, כמו גם שכנוע של בעלי עניין רבים. עם זאת, נראה שבפועל, פעמים רבות מתקבלות ההחלטות לא כמדיניות סדורה, אלא כ"כיבוי שרפות" והחלטות עקרוניות, או החלטות לטיפול מונע בגורמים מסוימים, נדחות.⁷⁸ כך או כך, יש להישמר מניסיון לשנות יותר מידי מהר מידי. התאמת הבירוקרטיה הממשלתית לפעולה במרחב הסייבר – כמו כל התאמה בירוקרטי - מחייבת שינויים איטיים והדרגתיים, תוך הבנת נקודות הקיבעון הקיימות במערכת הנוכחית. אין לנסות לערוך מהפיכות במערכת הקיימת.⁷⁹

תיאום

אחד מתפקידיה העיקריים של הממשלה הוא לתאם, הן בין מרכיביה השונים לבין עצמם והן בינם לבין המגזר הפרטי והאזרחים. בעניין זה, הצורך לתאם בין הגופים השונים הפועלים במרחב הסייבר אינו שונה מהצורך לתאם בין הגופים השונים הפועלים בתחומי ביטחון הפנים או המאבק בתאונות הדרכים. עם זאת, כיוון שמרחב הסייבר הוא מרחב חדש, לא תמיד קיימים הארגונים והתפקודים הנחוצים לתיאום בין הגופים השונים במרחב זה.

לדוגמה, בארה"ב, אין מקבילה ל-NSA/CYBERCOM הפועלת במרחב "הפנים מדינתי" הפדרלי\אזרחי, שאמורה לתאם את מאמצי כל הסוכנויות השונות הפועלות במרחב הסייבר. הסמכות שכן אמורה לתאם בין סוכנויות ממשלתיות שונות הפועלות במרחב הסייבר, נמצאת במועצה לביטחון לאומי והמשאבים העומדים לרשותה קטנים מידי (הסמכות כוללת מנהל אחד הממונה על ידי הנשיא ומספר קטן של אנשי מקצוע המגיעים ממגוון סוכנויות הביטחון ואורך תפקידם כשנתיים).⁸⁰

עם זאת, הצורך בפונקציה שכזו ברורה. לפי אסטרטגיית משרד ההגנה למרחב הסייבר, אמור משרד ההגנה להקים מסגרת ליכולות הסיוע האזרחי שלו (Defense Support of Civil Authorities). יכולות אלה אמורות לסייע למשרד להגנת המולדת ולסוכנויות אחרות בהגנה על הממשל הפדרלי והמגזר הפרטי בעת חירום – לפי פקודה. ההכרח לתאם עם סוכנויות אחרות לא מוגבל למקרים בהם משרד ההגנה הוא "המסייע", אלא גם למקרים של התקפה בעלת השלכות חמורות, בה משרד ההגנה הוא הגורם המוביל את המבצעים. עוד קובעת

⁷⁷ High Representative of the European Union for Foreign Affairs and Security Policy *Op. cit.*, p. 15-16

⁷⁸ David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, pp. 2-3, 52

⁷⁹ Richard J. Danzig, *Op. cit.*, p. 33

⁸⁰ Richard J. Danzig, *Op. cit.*, p. 33-34

אסטרטגיית משרד ההגנה האמריקני למרחב הסייבר שעל המשרד לבנות שיתוף פעולה בין גורמי הרכש, המודיעין, המודיעין המסכל, אכיפת החוק, המבצעים והמגזר הפרטי כדי למנוע אובדן מידע באמצעות מרחב הסייבר ולצמצם את נזקי מקרים אלה – כולל באמצעות סיוע ישיר לחברות העובדות על פרויקטים חיוניים לשפר את הגנותיהן.⁸¹

אף על פי כן, להקמת סמכות ריכוזית אחידה יש מספר בעיות:⁸²

1. מהלך ההקמה של סוכנות ריכוזית הוא ארוך ובעת הקמתה, ההתקדמות בכל המישורים היא קטנה מאוד.
2. סמכות חדשה תהפוך עד מהרה לקשיחה ומאובנת בדיוק כמו הסמכויות הקיימות כיום.
3. אפשר שהבעיה כלל אינה מצריכה סמכות יחידה, אלא עדיף לבנות יכולות הגנה במגוון הארגונים האזרחיים והציבוריים הקיימים כבר כיום. לכל ארגון שכזה נדרש פתרון ייחודי וסמכות מרכזית לא תיתן לכך מענה.

נראה גם שהקמת סמכות חדשה עשויה להביא ל"מלחמות בירוקרטיות" כיוון שהיא עשויה לפגוע בסמכויות של גופים קיימים. לכן, לעיתים, הסמכות המתאמת עשויה להיות מעט ריקה מתוכן. לדוגמה, בשנת 2014 קבע הקונגרס האמריקני שיוקם במשרד ההגנה תפקיד של יועץ עיקרי לשר ההגנה למרחב הסייבר (Principle Cyber Advisor). יועץ זה אמור לבחון את הפעילויות הצבאיות במרחב הסייבר, את כוחות המשימה למרחב הסייבר ואת המבצעים הצבאיים ההתקפיים וההגנתיים במרחב זה. עוד אמור היועץ להכווין את פיתוח המדיניות והאסטרטגיה של משרד ההגנה במרחב הסייבר עבור כלל גורמי המשרד. למעשה, אמור היועץ להיות גורם מתאם ומתכלל של גורמים בתוך משרד ההגנה ומחוצה לו כדי להבטיח פעולה טובה של המשרד וארגונו במרחב הסייבר. עם זאת, באסטרטגיית משרד ההגנה נקבע שהיועץ הנ"ל לא ישפיע על סמכויות קיימות בתחום עיסוקם במרחב הסייבר ולא ישמש ככפל סמכויות עם גורמים קיימים.⁸³ כך, אכן הוקמה סמכות תיאום חדשה, אך לא ברור מה הן סמכויותיה ובהיעדר סמכויות ברורות ועצמאיות, אפשר שאין טעם ברור בהקמתה כלל.

שיתוף מידע

כיוון שלמשתמשי הקצה תפקיד חיוני בהבטחת ביטחון הרשתות ומערכות המידע, יש ערך בשיפור מידת מודעותם לסיכונים ובהקניה להם של יכולת לנקוט בצעדים שיאפשרו להם

⁸¹ The Department of Defense Cyber Strategy, p. 22-25

⁸² Richard J. Danzig, *Op. cit.*, p. 33-34

⁸³ The Department of Defense Cyber Strategy, p. 29-30

להישמר מפני סיכונים אלה בעצמם.⁸⁴ כאמור, גילוי התקיפות במרחב הסייבר היא סוגיה בעייתית ורוב ההתקפות והפרצות לא מתגלות על ידי הגוף הנתקף ומכאן החשיבות של העברת מידע בין אלה שמסוגלים לגלות פרצות ובין אלה שנפלים קורבן לפרצות. סוגיית שיתוף המידע עם גורמי הממשל רלוונטית במיוחד לגופים פרטיים, כיוון שלגופים אלה יש פער בכל הנוגע למודיעין איומים "מערכתי" – משמע, מודיעין לגבי התקפות ספציפיות העתידות להתרחש כנגד הארגון. זאת מכיוון שהאמצעים והשיטות לאיסוף מודיעין מסוג זה אינם בידי הגופים הפרטיים - או שהן בלתי חוקיות כלל ועיקר - ומנגד, למדינה כלים, סמכויות ויכולות לאסוף ולהפיק מודיעין שכזה.⁸⁵ לדוגמה, גורמי מודיעין מדינתיים יכולים לסייע לחברות פרטיות לדעת מתי יריבים (בעיקר מדינתיים ומתוחכמים) הצליחו להשתיל פוגענים באתרי אינטרנט מסוימים, במטרה לפרוץ פרצות ברשתות של אותן חברות על ידי הדבקתן באמצעות עובדים שישוטטו באתרים אלה.⁸⁶ מחקרים שעורכים סוכנויות הביון עשויים גם לגלות מידע שסייע לחברות במגזר הפרטי לשפר את אבטחת מערכתיהם במרחב הסייבר לא רק על ידי בלימת התקפות בזמן אמת, אלא באמצעות שיפור את אבטחת מרחב הסייבר של אותן החברות באופן כללי. בהתאם, כל הגורמים, ובתוכם גם המגזר הפרטי יכולו להפיק תועלת רבה מגישה אוטומטית למגוון מקורות מידע – כולל "מסד נתונים לאומי לנקודות תורפה" (National Vulnerability Database) – כדי לאפשר להם לזהות בעצמם תורפות ולצמצמן בתוך זמן קצר.⁸⁷

הצורך לחלוק מידע בין גורמים הפועלים במרחב הסייבר הוא עניין מוכר. אסטרטגיית אבטחת מרחב הסייבר של האיחוד האירופאי טוענת שסוכנויות אבטחת המידע והרשתות הלאומיות נדרשות לשותף פעולה עם גורמי רגולציה אחרים – בייחוד סמכויות האמונות על אבטחת מידע אישי - ולחלוק עימם במידע.⁸⁸ אסטרטגיית משרד ההגנה למרחב הסייבר מכירה גם היא בצורך לפתח כלים אוטומטיים לשיתוף במידע (הן בין סוכנויות המדינה לבין עצמן והן בין לבין המגזר הפרטי) ולסייע לחקיקה ראשית שתקל על שיתוף המידע בין סוכנויות הממשל לבין המגזר הפרטי.⁸⁹

שיתוף מידע אינו תהליך גנרי. איומים שונים מצריכים שיתופי מידע (ופעולה) שונים בין צירים שונים ובין גורמים שונים בתוך הצירים האלה (לדוגמה, בין משרד ההגנה וספקי שירותי

⁸⁴ High Representative of the European Union for Foreign Affairs and Security Policy, *Op. cit.*, p. 7

⁸⁵ David Chismon and Martyn Ruks, *Threat Intelligence: Collecting, Analysing, Evaluating*, CPNI: MWR Infosec, 2015, p. 18

⁸⁶ Mandiant 2013 Threat Report - *M-Trend: Attack the Security Gap*, p. 11

⁸⁷ James A. Lewis, *Raising the Bar for Cybersecurity*, Center for Strategic and International Studies, 12 Feb. 2013, pp. 7, 11

⁸⁸ High Representative of the European Union for Foreign Affairs and Security Policy, *Op. cit.*, p. 6

⁸⁹ *The Department of Defense Cyber Strategy*, p. 25

האינטרנט, בין המשרד לביטחון המולדת וחברות אבטחה וכו). בהתאם לכך, זיהה ממשל אובמה חמישה צירים עיקריים לשיתוף מידע:⁹⁰

- בין סוכנויות הממשל הפדרלי לבין עצמן.
- בין סוכנויות הממשל הפדרלי לבין גורמי הממשל המקומי
- בין סוכנויות הממשל הפדרלי לבין ממשלות זרות
- בין סוכנויות הממשל הפדרלי לבין המגזר הפרטי
- בין גורמי המגזר הפרטי לבין עצמם

במגזר הפרטי יש מגוון דוגמאות לשיתופי מידע בין חברות (או לעיתים אף בין בעלי תפקידים ספציפיים בחברות) – בין השאר בין חברות העוסקות באבטחת מידע ובתקשורת. לעיתים אף מדובר בקבוצות ממוסדות ממש, שהחברות בחלקן מקבוצות מחייבת מיומנות ואף היכרות אישית וממליצים. במגזרים שונים, שיתוף המידע בענייני אבטחת מרחב הסייבר הוא תהליך ממוסד מזה שנים רבות. כך, בשנת 1998 פרסם הממשל הפדרלי האמריקני צו נשיאותי (PDD 63) שמטרתו הייתה לאפשר לממשל לעודד חברות פרטיות להקים גופים שבאמצעותם יוכלו לשתף מידע בתחום איומים במרחב הסייבר אחת עם השנייה (Information Sharing and Analysis Centers). בעקבות הצו, הוקמו מספר גופים שכאלה (בעיקר של גופי תשתיות לאומיות) – כגון זה המאגד את המגזר הפיננסי (FS-ISAC) ונחשב למוצלח מאוד, אם כי, לא כל המגזרים הצליחו במידה שווה.⁹¹ באופן כללי, סקר של חברת PwC שבחן את השוק האמריקני מצא שרק 25% מהחברות שהשיבו על הסקר היו שותפות במרכז שיתוף מידע זה או אחר בשנת 2014. עוד מצא סקר זה שהמגזרים בהם החברות בפורומים אלה הייתה מפותחת ביותר היו התשתיות החיוניות (מים וחשמל), הפיננסיים וסוכנויות הממשל. כיום יש מספר ניסיונות חקיקתיים להרחיב את שיתופי המידע בין חברות במגזר הפרטי (על ידי הגבלת החשיפה לתביעות כתוצאה משיתופי מידע) ויש כאלה הטוענים שמאמצים אלה ישפרו את השתתפות הגורמים השונים במיזמי שיתוף המידע.⁹²

גם במגזר הציבורי נערכו מגוון ניסיונות לשתף מידע – הן בין גופי הממשל לבין עצמם והן בין גופי הממשל לגופים פרטיים. במשרד לביטחון המולדת קיים גוף בשם National Cybersecurity and Communication Integration Center שמשמש כמרכז למודעות מצבית בנוגע לפעילות עוינת במרחב הסייבר. מרכז זה נועד לשתף מידע בין המגזר הפרטי, מפעילי השירותים החיוניים, וכל סוכנויות הממשל (כולל קהיליית המודיעין, גופי הביטחון ורשויות

⁹⁰ Jason Healey, *Op. cit.*, pp. 1-3

⁹¹ *Ibid*, pp. 1, 4-5

⁹² David Burg et. al., *Op. Cit.*, PwC, July 2015, p. 9

אכיפת החוק). גוף זה כולל בתוכו, בין השאר, את ה-CERT עבור הממשל הפדרלי ו-CERT עבור התשתיות החיוניות.⁹³ עוד מפעיל הממשל הפדרלי תוכנית לאיסוף, ניתוח ושיתוף מידע הנוגע לאבטחת מרחב הסייבר (תוכנית Einstein)⁹⁴ המיועדת לשרת את כל סוכנויות הממשלה הפדרלי.⁹⁵ בשנת 2007 הקימה ממשלת בריטניה גוף בשם Center for the Protection of National Infrastructure (CPNI) שתפקידו לייעץ לעסקים בבריטניה בנוגע לאבטחת מרחב הסייבר. גוף זה מקיים קשרי שותפות עם המגזר הפרטי הבריטי כדי לקדם את יישום הנחיותיו. גוף זה הוא חלק מארגון ה-MI-5.⁹⁶

על אף הבנת חשיבות הנושא והכרת הצורך, אפשר לטעון שבאופן כללי, המצב עדיין מצריך שיפור. כיום, נראה שמערך התמריצים והעלויות הקיים אינו מעודד את השיתוף במידע בין גופי הממשל לבין עצמם ובינם לבין המגזר הפרטי. בין השאר, מתבטא מערך תמריצים שלילי זה במספר דברים:⁹⁷

- האופן בו מסווג המידע שונה בין המדינה למגזר הפרטי - שחקנים במגזר הפרטי נדרשים להתחשב בסוגיות של חיסיון ופרטיות המידע האישי של לקוחותיהם ואילו הממשלה פחות מודאגת מסוגיות של פרטיות, נוטה לסווג מידע מבצעי רלוונטי בסיווג גבוה.
- הגנה משמעותית ושיטתית בזמן אמת עשויה לחייב סריקה של תוכן המידע הנכנס אל הרשת של הארגון – סריקה שהיא בעייתית לכשעצמה מבחינה חוקית, ולו מכיוון שמדובר במידע פרטי של המשתמשים שרובו נקי. סריקת תוכן המידע עשויה להיות אפשרית בארגונים כגון מקומות עבודה או שירותי הביטחון, אך הסריקה ברמה המדינתית היא בעייתית. לא זו אף זו, שיתוף של מידע זה – ועל אחת כמה וכמה עם רשויות אכיפת החוק והביטחון הלאומי – מפר את הפרטיות של המשתמשים באופן שעשוי להיות לא מידתי ביחס לאיום ולערך הנובע מהשיתוף, גם במקרים שהמידע

⁹³ National Cybersecurity and Communications Integration Center, www.dhs.gov/national-cybersecurity-communication-integration-center

⁹⁴ תוכנית Einstein סורקת את כל המידע שנכנס ויוצא מהרשתות שנמצאות בהגנת המשרד לבטחון המולדת. התוכנה סורקת את הכותרת של כל מנה, אך לא את תוכנה, ומשווה את התוצאות עם דפוסים מוכרים שכבר יוחסו לנוזקות.

David Clarck, Thomas Berson and Herbert S. Lin (eds.), **Op. cit.**, p. 37

⁹⁵ Privacy Impact Assessment Einstein Program – Collecting, Analyzing and Sharing Computer Security Information across the Federal Civilian Government, Washington, DC: Department of Homeland Security, National Cyber Security Division – Computer Emergency Readiness Team, p. 1

⁹⁶ James A. Lewis, **Raising the Bar for Cybersecurity**, Center for Strategic and International Studies, 12 Feb. 2013, p. 9

⁹⁷ Jason Healey, **Op. cit.**, pp. 2-4; James A. Lewis, **Op. cit.**, p. 6; Mandiant 2013 Threat Report - **M-Trend: Attack the Security Gap**, p. 26; David Clarck, Thomas Berson and Herbert S. Lin (eds.), **Op. cit.**, p. 67-68

- הוא מידע של ארגונים ולא של משתמשים פרטיים. סוגיה זו מוטלת לפתחה של המדינה ועליה לקבוע איזה מידע מותר לסרוק, כיצד ואיך לשתפו – אם בכלל.
- מערכות המידע המשמשות את הגורמים השונים לא תמיד תואמות ועלות הקמת מערכות ייעודיות או שיפור התאימות בין המערכות הקיימות גבוה.
 - ישנו פער של אמון בין הגורמים המקשה על שיתוף המידע. חברות במגזר הפרטי – בייחוד חברות הרב-לאומיות – לא תמיד מסוגלות לבטוח בממשלות ובארגוני הביון שלא ישתמשו בנהלים ובשיפורי האבטחה שהנהיגו בארגונים פרטיים שונים לשם עקיפת האבטחה שלהן⁹⁸ ולא יכולות תמיד לתת אמון בכך שהמידע שהמדינה משתפת אותם הוא מלא, עדכני או נכון.
 - כאשר ממשלות וגורמים פרטיים כן משתפים מידע, השיתוף לרוב מתקיים בתוך גבולות המדינה, למרות שהסוגיות הן גלובליות.
 - כמו כן, במידה רבה אפשר לראות שכאשר שיתוף מידע כן מתרחש, פעמים רבות הוא מתרחש בין אנשים ספציפיים שחברים בארגונים הללו ויש בניהם היכרות אישית ואמון. שיתוף מידע שנערך באופן זה חשוף לסכנות הנובעות מתנועות כוח האדם בארגונים השונים.
 - יש כאלה המפקפקים ביעילות שיתוף המידע. לטענתם, כיוון ששיתוף במידע בין הממשלה למגזר הפרטי הוא הליך סביל, המתרחש לאחר התקפה, אין בו די כדי לעצור את כל ההתקפות – ועל אחת כמה וכמה התקפות לא מוכרות שנמצאות בעיצומן – לא כל שכן בהתחשב במהירות האיטית של התהליכים הביורוקרטיים ביחס למהירות הגבוהה של ההתקפות במרחב הסייבר.
 - יש מתח מובנה בבחירה לפרסם מודיעין ולשתפו. מחד גיסא, המודיעין יכול לסייע רבות בהתמודדות עם תוקפים – במיוחד אם מדובר בתוקפים גדולים וממוסדים. מאידך גיסא, המודיעין עשוי לסייע לתוקף להבין שהוא זוהה ואף להתמודד עם גורמי המודיעין וכך להקשות על המשך המעקב אחריו.
 - פרסום מידע על איומים במרחב הסייבר עשוי לחשוף את הגורם המפרסם לתקיפה – על אחת כמה וכמה אם גורם זה הוא גורם פרטי.
- עידוד שיתוף מידע (ופעולה) בין הגורמים השונים הפועלים במרחב הסייבר בכל הנוגע לאבטחת מרחב הסייבר יכול להיערך במספר דרכים. הממשלה יכולה להסדיר סמכויות משפטיות וגורמים אחרים בחקיקה, להשקיע כסף בעידוד חברות פרטיות לשתף פעולה, לעמוד בקשר עם ממשלות זרות, להיות חברה בפורומים עם גורמים לא מדינתיים, להקים

⁹⁸ בדומה למה שגילו ההדלפות של אדוארד סנאודן.

ארגוני שיתוף פעולה ומידע ומסדי נתונים רלוונטיים ושיתופיים, ליצור משרות ספציפיות במשרדי הממשלה ובסוכנויות הממשל שיעודדו שיתוף במידע (לדוגמה על ידי הבטחת הורדת סיווג מהירה של המידע והפצתו) וליצור יעדים ותוכניות ברורות לתגובה ושיתוף פעולה שישימו כמטרה השגת תוצאה ולא שיתוף מידע (או פעולה) לכשעצמו. כך או כך, בראש ובראשונה יש לזכור שעל שיתוף המידע להיות כלי להשגת תוצאה (עצירת תקיפה או סגירת נקודת תורפה, לדוגמה) ולא מטרה לכשעצמו.⁹⁹

שיתוף המידע לא נדרש להיות חד כיווני (מהמדינה אל המגזר הפרטי), אלא דו כיווני ואף רב כיווני. שיתוף פעולה עם חברות אזרחיות – בעיקר עם חברות אבטחה במרחב הסייבר – לא בהכרח מצריך הסכמים מורכבים, אלא רק "מספר כרטיס אשראי". המדינה יכולה לשלם עבור מידע (לדוגמה – קניית תורפות יום אפס [Zero Day Vulnerability])¹⁰⁰ ועבור שירותי אבטחה אחרים במרחב הסייבר.¹⁰¹ עם זאת, גם שיתוף פעולה בסיסי זה עשוי לחייב שינויים בנהלי המכרזים.

שיתוף במידע לא נוגע רק לסיכול איומים, אלא גם לשיפור מודעות של הגורמים השונים לתהליכים ואיומים במרחב הסייבר. אחד מהתפקידים העיקריים של המדינה בכלל ושל מקבלי ההחלטות בה בפרט הוא להעלות את המודעות – הן בציבור הרחב והן בארגונים השונים (גם במגזר הפרטי וגם במגזר הציבורי) – בנוגע לאתגרי אבטחת מרחב הסייבר. שיפור מודעות זה נדרש כדי לשנות את משוואת הרווח וההפסד של הגורמים השונים ולעודדם לשים דגש רב יותר על אבטחת מרחב הסייבר – הן בהתנהגותם כיחידים, כארגונים וכחלק ממערכת כוללת והן במוצרים ובטכנולוגיות שהם מפתחים – למרות העלויות (שלעיתים אינן מבוטלות) הכרוכות בכך בטווח הקצר. לא זו אף זו, המדינה נדרשת לרתום באופן פעיל את המגזרים השונים במדינה (ומחוצה לה) לטובת שיפור אבטחת מרחב הסייבר כולו ולא רק לטובת שיפור אבטחת מרחב הסייבר של הארגונים כיחידים.¹⁰² לפיכך, המדינה יכולה להיות גורם שמרכז ידע עבור האזרחים והמגזר הפרטי בצורה נגישה ומובנת. כמו כן, המדינה יכולה להיות גורם המפתח ידע רלוונטי¹⁰³ – אם בעצמה ואם באמצעות מלגות מחקר לגורמים חיצוניים – עבור האזרחים ועבור גורמים במגזר הפרטי שאינם יכולים להרשות לעצמם פיתוח ידע ארגוני עצמאי בתחום אבטחת מרחב הסייבר.¹⁰⁴

⁹⁹ Jason Healey, *Op. cit.*, pp. 5-6

¹⁰⁰ וגם לגבות תשלום עבור חלק משירותי האבטחה שהיא מספקת, כגון חברות במאגר נתונים לאומי לנקודות תורפה. כמובן, שימוש במגזר הפרטי (החוקי והבלתי חוקי) על ידי המדינה במרחב הסייבר יכול להיות למטרות התקפיות ולא רק הגנתיות.

¹⁰¹ Jason Healey, *Op. cit.*, p. 7; *The Department of Defense Cyber Strategy*, p. 10

¹⁰² David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, p. 80

¹⁰³ בדומה למרכז לשליטה במחלות ומניעתן (CDC) של הממשל הפדרלי האמריקני.

¹⁰⁴ P. W. Singer, *Op. cit.*

בשאלת מידור המידע אל מול שיתופו, אפשר לקבוע שגורמים אזרחיים שונים יחשפו למידע שונה לפי הצורך. באופן כללי, המידע המסווג הוא לרוב מידע "מערכתי"¹⁰⁵ או אף טקטי ואינו תורם באופן מהותי לדיון "האסטרטגי" על המדיניות הכללית של ההגנה או ההתנהלות במרחב הסייבר. כך, אפשר להכריע שמודעות הציבור והדיון הציבורי צריכים להתרכז ברמה "האסטרטגית" (הכוללת, לרוב, מידע הגלוי ממילא), בעוד שמודעות הארגונים השונים צריכה לנוע מהרמה האסטרטגית (של מקבלי ההחלטות), דרך הרמה המערכתית ועד הרמה הטכנית – בהתאם לעיסוק כל גורם וגורם. עוד אפשר לקבוע, לדוגמה, שתפקיד של המדינה הוא לעודד מודעות בקרב הגורמים השונים ברמה האסטרטגית ולתרגל את כל הגורמים ברמה זו, להתריע בפני גורמים רלוונטיים על מידע "מערכתי" קיים (לפי מגבלות הסיווג וכו') ולחלוק במידע ברמה הטקטית והטכנית באמצעות ריכוז המידע הקיים אצל הגורמים השונים במאגר מידע מרכזי.

סוגיה ספציפית שיש לדון בה בכל הנוגע לשיפור המודעות היא הסוגיה ההתקפית. יכולות התקפיות עשויות לסייע באופן זה או אחר בהגנה במרחב הסייבר. עם זאת, אופיין המסווג של יכולות אלה עשוי לחבל במידת ההבנה של הגורמים השונים את תרומתם ואת השפעתם הרחבה יותר. מכאן, אולי יש מקום לבחון את מידת הסיווג ואף את הצורך בסיווג של יכולות התקפיות שונות במרחב הסייבר לאור התועלת הציבורית הנרחבת יותר (אם קיימת כלל) שעשויה להיות לחשיפתן (במידה זו או אחרת). בהקשר זה, מחקר אמריקני חילק את רגישות המידע על יכולות התקפיות לשלושה סוגים:¹⁰⁶

- עצם העניין בטכנולוגיה מסוימת ככלי התקפי.
- פרטים מבצעיים שאינם טכנולוגיים בעיקרם (קיומה של פרצה ספציפית במדינה ספציפית כלשהיא או של תוכנית מבצעית מסוימת).
- הכרת יכולת מסוימת או כוונה מסוימת של היריב.

בהקשר זה, אסטרטגיית מרחב הסייבר של משרד ההגנה מפרטת באופן כללי, אך ברור, שארה"ב "תערוך מבצעים במרחב הסייבר" (כלומר – תתקוף במרחב הסייבר) כדי לבלום התקפה במרחב הסייבר העתידה להתרחש בעתיד הקרוב מאוד (Imminent) או הנמצאת בעיצומה כנגד ארה"ב או האינטרסים שלה, זאת, לרוב, רק לאחר מיצוי הגנות הרשת

¹⁰⁵ סוכנות ה-CPNI הבריטית מבדילה בין ארבע רמות של מודיעין איומים – אסטרטגי (מידע "ברמה גבוהה", לא טכני, על איומים המיועד למקבלי ההחלטות), מערכתי (פרטים על התקפות ספציפיות העתידות להתרחש, המיועד לאנשי אבטחת מידע בכירים), טקטי (מתודולוגיות, כלים וטקטיקות, מיועד ל"אנשי השטח" של מערך אבטחת הסייבר) וטכני (אינדיקטורים של כלים ספציפיים כגון גיבוי MD5 של נזקות ספציפיות). חלוקה זו עשויה להועיל להסדרה של סוגי המידע שיש להעמיד כגלוי לגורמים השונים. לעניין חלוקת רמות מודיעין האיומים הבריטית ראה:

David Chismon and Martyn Ruks, **Op. cit.**, pp. 6-7

¹⁰⁶ David Clark, Thomas Berson and Herbert S. Lin (eds.), **Op. cit.**, p. 3

ואפשרויות הפעילות במסגרת כלי אכיפת החוק. עוד טוענת האסטרטגיה שארה"ב תחזיק ביכולות התקפיות במרחב הסייבר כחלק מיכולותיה הצבאיות, עד כדי יכולת לסיים עימות קיים תוך יתרון לארה"ב, אך שהיא תפעל תוך איפוק ופיקוח, לאחר דיון מעמיק, "בהתאם לערכיה של ארה"ב" ובהתאם לדיני המלחמה.¹⁰⁷

עם זאת, בכל נושא השיתוף במידע יש לאזן את הסיכונים והתועלת הנובעים מחשיפה רבה יותר של מידע ומודיעין הנוגעים בסיכונים ובאיומים במרחב הסייבר.¹⁰⁸ כדי למנוע דליפה של המודיעין ליריב, על השיתוף להיעשות בתנאים מסוימים כלומר, בקבוצות סגורות (אפשר בקבוצות הייחודיות למגזרים שונים במשק) בהן קיים אמון חזק בין המשתתפים. הממשלה או סוכנויותיה השונות יכולים להיות הגורמים אשר יקימו ו\או יקדמו קבוצות שכאלה – כמו שעושים גופים שונים בממשלה הבריטית – ואף להיות הגורם שמטשטש את זהות החברות המשתפות מידע כדי למנוע פגיעה בהן.¹⁰⁹

¹⁰⁷ **The Department of Defense Cyber Strategy**, pp. 5-6

¹⁰⁸ Richard J. Danzig, **Op. cit.**, p. 23

¹⁰⁹ David Chismon and Martyn Ruks, **Op. cit.**, p. 11

בניין כוח - פיתוח ידע, הכשרה, כוח אדם וארגון

פיתוח ידע

מרחב הסייבר מצריך בניין כוח שיאפשר פעולה בו ובאמצעותו. עקב חדשנותו של מרחב הסייבר, פער מרכזי במסגרת תהליך בניין הכוח לפעולה במרחב הסייבר, הוא בראש ובראשונה פיתוח ידע בנוגע למרחב זה.

יש הטוענים שפערי הידע הקיימים בכל הנוגע למרחב הסבר, הם ניכרים. כך, לדוגמה, נשמעות טענות שכיום אפילו לממשל האמריקני אין הבנה מוצקה של הסיכונים המתקבלים על הדעת והבלתי מתקבלים על הדעת בכל הנוגע לפעילותו במרחב הסייבר, כמו גם הבנה של תפקידי הממשל ותפקידי המגזר הפרטי במרחב זה.¹¹⁰ נוסף על כך, ישנם נטען שקיימים גם פערי ידע בנוגע לעצם הדינמיקה של הסלמה והרתעה במרחב הסייבר - בעוד שמודלים קיימים להסלמה והרתעה בהם נעשה שימוש (באופן גלוי, לפחות) נגזרים בעיקר מהרתעה גרעינית ואין ביטחון בהתאמתם למרחב הסייבר. לפיכך, המדינה נדרשת לפתח ידע בנוגע לסוגיית ההסלמה וההרתעה במרחב הסייבר – תוך שיתוף פעולה עם האקדמיה ועם המגזר הפרטי.¹¹¹ דוגמה למאמץ פיתוח ידע מסוג זה היא העבודה של כוח המשימה של וועדת המדע לענייני הגנה העוסקת בהרתעה בסייבר (Defense Science Board's Task Force on Cyber Deterrence).¹¹² צמצום הפער הקיים היום בתחום אבטחת מרחב הסייבר מחייב שני סוגים של מחקר ופיתוח – הראשון, מחקר בסיסי (לא טכני ברובו) בנוגע לאופן בו יש ליישם טכנולוגיות וטכניקות קיימות כדי לאבטח טוב יותר את מרחב הסייבר. השני, מחקר ופיתוח (גם טכני) בנוגע לטכנולוגיות חדשות וטכניקות חדשות (כולל מבנים ארגוניים, סמכויות וכו') שישפרו את אבטחת מרחב הסייבר כיום ובעתיד הנראה לעין (גם כנגד איומים אפשריים עתידיים). מאמץ המחקר והפיתוח נדרש להיערך בשני מישורים:¹¹³

- מחקר מכוון בעיה ספציפית שנדרש למצוא פתרון נקודתי לבעיה נקודתית – כולל בחינה של האופן בו ניתן להפעיל פתרונות קיימים נגד בעיות ידועות.
- סגירת הפער הכללי הקיים בין המגן לבין התוקף בעל היכולות הגבוהות (או במילים אחרות, צמצום העליונות המובנית של התוקף במרחב הסייבר).

כחלק מתהליכי המחקר, נדרש טיפול בפער הידע האמין הקיים בנוגע לתורפות ולהתקפות במרחב הסבר. פער זה מתקיים עקב מגוון סיבות, בין השאר היעדר נכונות של גורמים שונים

¹¹⁰ Richard J. Danzig, *Op. cit.*, p. 19

¹¹¹ David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, p. 77

¹¹² *The Department of Defense Cyber Strategy*, p. 25

¹¹³ *Ibid*, pp. 61, 79-80

לדון בתורפות ובהתקפות במרחב הסייבר. המדינה יכולה להיות הגורם המתעדף מחקר בכיוון זה.¹¹⁴ עם זאת, אופי מרחב הסייבר מביא לכך שמחקר מבוזר יותר ותחרותי יותר עשוי להיות עדיף על מחקר ריכוזי – גם במחיר יעילות. בהתאם, יש הטוענים שבניגוד לדחף הראשוני של המדינה לעבר הפעלה ריכוזית של סמכויות, כדאי להימנע מהדחף להכווין באופן ריכוזי את כל המחקר בתחום הסייבר (גם זה הממשלתי).

בעוד שבעבר הייתה המדינה בכלל והכוחות המזוינים בפרט כוח מניע בתהליך המחקר והפיתוח האזרחי,¹¹⁵ כיום תקציבי המחקר והפיתוח של חברות ההיי-טק הגדולות גדולים יותר מאשר תקציבי הביטחון של מדינות רבות.¹¹⁶ לפיכך, בבניין הכוח הן של הצבא והן של המדינה בכלל, יש צורך להסיט את המיקוד מפיתוח של טכנולוגיות לפיתוח של אמצעים ספציפיים¹¹⁷, להקמה של רשתות מאובטחות על בסיס טכנולוגיות אזרחיות ובמיוחד לשיפור של טכנולוגיות מדף קיימות (לדוגמה - סגירת פרצות במערכות הפעלה אזרחיות שבשימוש הצבא והמדינה או לשיפור הגנת הסייבר של אמל"ח קיים). הדבר מצריך שינויים רבים בצורת החשיבה הן של המדינה והן של הצבאות, הרגילים לפעול על בסיס טכנולוגיה ייעודית. בתוך כך נדרשים שינויים בנהלי הרכש, בדרך בה המדינה יוצרת קשר עם גורמים אזרחיים, בקצבי בניין הכוח ועוד. זאת משום שטכנולוגיית המידע מתעדכנת בקצב מהיר הרבה יותר מאשר הטכנולוגיות הצבאיות המסורתיות ומפותחת על ידי חברות שאינן מורגלות לעבוד עם הבירוקרטיה הסבוכה של המדינה.¹¹⁸ מנגד, הממשלה יכולה וצריכה למקד את המחקר בנושאים הבסיסיים של

¹¹⁴ Richard J. Danzig, *Op. cit.*, pp 54-55

¹¹⁵ לדוגמה – רבות מהטכנולוגיות הנמצאות בבסיס הטלפון החכם פותחו לראשונה על ידי סוכנות DARPA האמריקנית. ראה:

Pierre Blenaine, "This Chart Shows How The US Military Is Responsible for Almost All the Technology in your iPhone", *Business Insider*, 29 Oct. 2014, www.businessinsider.com/the-us-military-is-responsible-for-almost-all-the-technology-in-your-iphone-2014-10

Loren Thompson, "Five Reasons Why Silicon Valley Won't Partner With the Pentagon", *Forbes*, 27 Apr. 2015, www.forbes.com/sites/lorenthompson/2015/04/27/five-reasons-why-silicon-valley-wont-partner-with-the-pentagon/

¹¹⁶ לדוגמה, תקציב המחקר והפיתוח של סמסונג בשנת 2013 עמד על 13.4 מיליארד דולר, של אינטל על 10.6, של מייקרוסופט 10.4 מיליארד דולר ושל גוגל 8 מיליארד דולר. ראה:

Michael Casey and Robert Hackett, "The Biggest R&D Spenders Worldwide", *Fortune*, 17 Nov. 2014, www.fortune.com/2014/11/17/top-10-research-development/; Brad Reed, "Samsung is Spending an Insane Amount of Money to Beat Apple to the 'Next Big Thing'", *BGR*, 10 Mar. 2015, www.bgr.com/2015/03/10/samsung-r-and-d-spending-2014/

¹¹⁷ בהינתן העלויות ומשכי הפיתוח של החומרה, אפשר שיעקר פעילות הפיתוח העצמאית של הצבא והמדינה יעשו בתחום התוכנה.

¹¹⁸ לעניין זה ראה דבריו של שר ההגנה האמריקני אשטון קרטנר בנאומו באוניברסיטת סטאנפורד באפריל 2015: Ashton B. Carter, "Rewriting the Pentagon: Charting a New Path on Innovation and Cybersecurity", *Defense.gov*, 23 Apr. 2015, www.defense.gov/News/Speeches/Speech-View/Article/606666/drell-lecture-rewriting-the-pentagon-charting-a-new-path-on-innovation-and-cyber

אבטחת מרחב הסייבר ולא להסתפק בשיפורים הדרגתיים המוצעים על ידי כוחות השוק הפרטי. זאת באמצעים הבאים:¹¹⁹

- מיפוי, במידת האפשר, של ההשקעות הממשלתיות והפרטיות באבטחת מרחב הסייבר כדי להבין את תמונת המצב בתחום.
- זיהוי הזדמנויות קריטיות לשיפור מהותי של אבטחת מרחב הסבר ותמרוץ מאמצים בכיוון זה הן במגזר הפרטי והן במגזר הממשלתי – תוך הימנעות מניסיון לתאם באופן הדוק את כלל ההשקעות השונות במשק.

עם זאת, אין זה הגיוני להניח שהמחקר לבדו ישפיע באופן משמעותי על האיומים בסייבר. המחקר והפיתוח הם עוד כלים בתהליך בניין הכוח - תהליך שעליו להיות רחב יריעה, מתמשך ולערב גורמים רבים בעלי עניין – הן ממשלתיים והן אזרחיים.¹²⁰

ארגון

יש הטוענים שלשם בניין כוח לפעולה במרחב הסייבר נדרשים ארגונים ייעודיים, עם אתוס ותרבות מתאימים, ארגון מתאים, שיטות בניין כוח מתאימות ומדיניות מתאימה.¹²¹ זאת לא רק עקב סוגיות כוח אדם, אלא גם עקב סוגיות של הפעלת הכוח - בין השאר, מכיוון שהכנסת תחום הסייבר לארגון קיים עשויה לגרום להטיה ביכולותיו הקיימות. כך, יש הטוענים שבארה"ב, בה פיקוד מרחב הסייבר (CYBERCOM) מאוחד עם סוכנות הביטחון הלאומית (NSA), יש הטיה ברורה של מאמצי הסייבר לכיוון המודיעיני (הן בהיבטי תעדוף המאמצים והמשאבים והן בהיבטי הקידום ומדיניות כוח האדם), עקב החוזק הבירוקרטי וה"עליונות הכרונולוגית" של ה-NSA. כמו כן, האופי הצבאי של שני הגופים מתעדף את ההתקפה על פני ההגנה. לפיכך, יש אף הטוענים שנדרשת הפרדה בין שני הגופים – המלצה שנדחתה עד כה.

122

דוגמה להקמת ארגונים חדשים לשם פעולה במרחב הסייבר אפשר לראות בתהליך בניין הכוח של הכוחות המזוינים האמריקניים. אלה נמצאים כיום בעיצומו של תהליך בניין כוח להקמת כוחות משימה למרחב הסייבר (Cyber Mission Forces). כוחות אלה יתחלקו לשלושה סוגים – כוחות הגנה בסייבר (Cyber Protection Forces) האמונים על הגנת הרשתות הצבאיות; כוחות המשימה הלאומיים (National Mission Forces) האמונים על הגנת ארה"ב מפני התקפות סייבר בעלות השלכות משמעותיות; וכוחות משימה לוחמים (Combat mission Forces)

¹¹⁹ *Ibid*, p. 31-32

¹²⁰ David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, p. 62

¹²¹ Gregory Conti and John "Buck" Surdu *Op. cit.*, p. 16

¹²² Richard J. Danzig, *Op. cit.*, p. 33

האמורים לשמש את מפקד הפיקוד האסטרטגי (Combatant Commander) בתפקודים שאינם הגנתיים ולסייע לו במשימותיו.¹²³ בדומה לכך וככל הנראה כפועל יוצא מתהליך זה, הקים הצי האמריקני "חיל עליונות המידע" (Information Dominance Corps) שמאגד תחתיו את הלוחמה האלקטרונית ושאר לוחמת המידע. צבא היבשה שוקל להקים גם הוא חיל דומה. בינתיים, איחד צבא היבשה את גורמי התו"ל העוסקים בלוחמה אלקטרונית, קשר ומבצעים במרחב הסייבר ב"מרכז המצוינות למרחב הסייבר" (Cyber Center of Excellence), בפורט גורדון.¹²⁴ כך אנו רואים תהליך בו הכוחות המזוינים מקימים ארגונים חדשים לחלוטין, השונים במידה ניכרת מארגונים קיימים (לדוגמה – על ידי הפרדה בין ההגנה להתקפה או על ידי ייחוד צוותים ספציפיים לעיסוק בהגנה ברמה הלאומית), אך תוך כדי כך, מנסים לשלב אותם בארגון הקיים הן במהלך בניין הכוח (אחריות בניין הצוותים חולקה בין הזרועות הקיימות) והן מבחינת הפעלת הכוח (חלק מהצוותים ימצאו בפיקוד המפקד האסטרטגי ואילו חלק מהם ימצאו בפיקוד הישיר של פיקוד מרחב הסייבר האמריקני).

כוח אדם והכשרה

סוגיה משמעותית נוספת בנוגע לבניין הכוח במרחב הסייבר היא סוגיית כוח האדם. בארה"ב (כולל בסוכנות לביטחון לאומי של ארה"ב - NSA - National Security Agency) מסתמנים כיום מספר פערים בנוגע לכוח האדם הזמין לפעולה במרחב הסייבר. פער אחד הוא פער הבנה ומקצועיות בין הדרג הזוטר לדרג מקבלי ההחלטות. המצב כיום הוא שהדרג הבכיר – הגם שמכיר במידה מסוימת את מרחב הסייבר – אינו מומחה בתחום ומבוגר בגילו. דרג זה ממונה על דרג זוטר, צעיר ומומחה בתחום. מצב זה גורם לכך שאין דרג ביניים בין שני הדרגים ויש שיעור נשר גדול מאוד בקרב הדרג הזוטר לטובת המגזר הפרטי – לעיתים קרובות אחרי משך שירות קצר מאוד בתפקיד. הסביבה הארגונית הממשלתית, כמו גם נהלי כוח האדם הממשלתיים אינם מתאימים לגיוס וטיפוח של כוח אדם בעל מיומנות בתחום מרחב הסייבר (החל מתחום הנתונים למשרה וכלה בתחום התגמול והלבוש) – על אחת כמה וכמה כוח אדם איכותי מאוד, בהינתן התחרות עם המגזר הפרטי. לא זו אף זו, הנהלים הקיימים מפריעים למעבר החופשי של כוח אדם בין המגזר הפרטי והציבורי ובין משרות שונות במגזר הציבורי. במגזר הציבורי (לפחות האמריקני), כוח האדם לאבטחת במרחב הסייבר מסווג אף ככוח אדם שעובד בתחום שהוא תחום משנה טכנולוגיית המידע, למרות שמדובר בתחומי עיסוק שונים במגזר הפרטי. בעוד שה-NSA מסוגל להתמודד עם המגזר הפרטי על ידי סמכויות כוח אדם

¹²³ **The Department of Defense Cyber Strategy**, Washington, DC: Department of Defense, 17 Apr. 2015, p. 6

¹²⁴ Isac R. Porche, "Cyberwarfare Goes Wireless", **RAND**, Apr. 4 2014, www.rand.org/blog/2014/04/cyberwarfare-goes-wireless.html

מיוחדות, הילה מקצועית, ציוד ייחודי ומסה קריטית של מומחים מהשורה הראשונה בתחום, סוכנויות אחרות אינן מסוגלות להתחרות עם השוק הפרטי באותו האופן.¹²⁵

סוגיית כוח האדם היא סוגיה בעייתית לא רק בממשל באופן כללי, אלא גם בתוך הכוחות המזוינים האמריקניים באופן ספציפי. יש הטוענים שהזרועות הקיימות של הכוחות המזוינים האמריקניים אינן מתאימות לבניין כוחות לפעולה במרחב הסייבר, בעיקר בגלל פערים תרבותיים שאינם מאפשרים גיוס, פיתוח, קידום, תגמול וניהול של כוח האדם בעל היכולות המתאימות בפרט ושל יכולות רלוונטיות בכלל. האתוס של הזרועות השונות, הידע והמיומנויות של הדרגים הבכירים בהם כלל אינו מתאים לאתוס, לידיע ולמיומנויות הדרושים לבניין כוח לפעולה במרחב הסייבר. זאת משום שהמהות של הזרועות הקיימות הוא בניין כוח מסוג מסוים לפעולה במרחב הפיזי ומהות זו משפיעה על כל פעולותיה – החל מרכש, דרך מעמד חברתי וכלה ממדיניות קידום ותגמול כוח אדם. בהתאם, יש הטוענים שאי אפשר ואף לא צריך לשנות את המהות הזו והתרבות, הארגון והאתוס הנלווים אליה ובמקום, נדרש לבנות ארגונים חדשים לגמרי לבניין כוח לפעולה במרחב הסייבר. אפילו הסוכנות הביטחון הלאומית של ארה"ב, העוסקת במידה זו או אחרת בפעולה במרחב הסייבר, אינה מתאימה לבניין כוח לפעולה במרחב זה – בעיקר עקב הקשיים שכופה מדיניות כוח האדם הצבאית (לדוגמה, תקופות שירות קצרות של קצינים בתפקיד ומעבר תכופ של קצינים בין תפקידים שונים בתכלית).¹²⁶

כל זאת יש להוסיף את מצוקת כוח האדם הכללית הקיימת בתחום אבטחת המידע – כבר היום, כ-40% ממשרות אבטחת הסייבר בבולשת הפדרלית האמריקנית (FBI) אינן מאוישות ועד 2020 צופים שהפער העולמי בין כמות משרות אבטחת מרחב הסייבר הפתוחות לבין כוח האדם הזמין יעמוד על כ-1.5 מיליון משרות פתוחות.¹²⁷

לסוגיית כוח האדם עשויות להיות מגוון פתרונות. עבור הממשלה עצמה, עשויות הפתרונות להיות די פשוטים. לדוגמה, הצבא וסוכנויות ממשל אחרות יכולים להשתמש במערך המילואים לשם ניצול כוח אדם בעל הכשרת סייבר אזרחית. כך, חיילי מילואים בעלי הכשרה ומיומנויות שנרכשו באזרחות יוכלו לעבור לשרת ביחידת סייבר במילואים ללא קשר לשירותם הסדיר – בדומה למצב הקיים אצל רופאים.¹²⁸ כמו כן, אפשר שמכון מחקר ממשלתי ייעודי – בעל מדיניות כוח אדם ייעודית, תרבות ארגונית ייעודית ובניהול אדם בעל מומחיות אמיתית בתחום – יוכל להגביר את יכולת הגיוס והשימור של המגזר הציבורי בכל הנוגע לתחום מרחב הסייבר.

¹²⁵ Richard J. Danzig, *Op. cit.*, p. 34-35

¹²⁶ Gregory Conti and John "Buck" Surdu, "Army, Navy, Air Force and Cyber – Is It Time for a Cyberwarfare Branch of Military?", *IAnewsletter*, Vol. 12, No. 1, Spring 2009, pp. 14, 16

¹²⁷ P. W. Singer, *Op. cit.*

¹²⁸ דגם דומה נהגה בארה"ב, שם הסב המשמר הלאומי מספר יחידות קיימות ליחידות סייבר. ראה: P. W. Singer, *Op. cit.*,

מרכז מחקר זה יוכל לשרת את כל סוכנויות הממשל (גם על ידי "השאלת" מומחים לפרויקטים ספציפיים), להיות גורם שיכשיר כוח אדם שכבר עובד בגורמי הממשל השונים ואף להיות הגורם שיקשר בין מומחים במגזר הפרטי לבין מומחים במגזר הציבורי.¹²⁹

אך יש לזכור שסוגיית מרחב הסייבר אינה ביטחונית בלבד, אלא שלמדינה אינטרס לפתח כוח אדם בעל מיומנויות אבטחה ופעולה במרחב הסייבר לא רק עבור מוסדותיה באופן ישיר, אלא עבור המשק באופן כללי.¹³⁰ לפיכך, המדינה יכולה להיות גורם המסדיר את תכני ההכשרה של אנשי הסייבר ומפקחת על איכות ההוראה בכל המשק, זאת בדומה למתרחש במקצוע הרפואה - על אחת כמה וכמה עקב הסוגיות האתיות והחוקיות הקשורות בתחום "ההתקפה בסייבר".¹³¹ המדינה יכולה להיות גם גורם שמעודד את מיומנויות הסייבר בקרב ילדים, תלמידי תיכון וסטודנטים - בין השאר על ידי תחרויות (בדומה לתחרויות ספורט), מלגות, התמחויות ותוכניות אחרות. בהקשר זה, ראוי לציין שסוגיות אבטחה במרחב הסייבר נוגעות לכל האזרחים ושיפור התנהלות האזרח במרחב הסייבר תשפר את אבטחת מרחב הסייבר באופן כללי - בין אם ע"י צמצום הפגיעות של הגורמים השונים במדינה לכל מיני שיטות חדירה ובין אם על ידי צמצום הפאניקה (והנזקים) בעת התקפה בסייבר. מכאן, שלמדינה עשוי להיות אינטרס משמעותי בשיפור החינוך להתנהלות נכונה במרחב הסייבר (הן בהיבט המודעות לאבטחה בסייבר והן בהיבט ההתנהגות הנכונה בסייבר) - כשם שיש לה אינטרס לשיפור החינוך בנושאים אחרים (הגיינה, אכילה נכונה, שמירה על הטבע, זהירות בדרכים וכו.). פרויקטים אלה, שידרשו להיות מוטמעים בקרב כל שכבות האוכלוסייה, ידרשו תיאום של גורמי הסייבר עם גורמי החינוך השונים.¹³²

¹²⁹ Richard J. Danzig *Op. cit.*, p. 35

¹³⁰ P. W. Singer, *Op. cit.*

¹³¹ Daniel Manson and Ronald Pike, "The Case for Depth in Cybersecurity Education", *ACM Inroads*, Vol. 5, No. 1, March 2014, p. 47

¹³² David Clarck, Thomas Berson and Herbert S. Lin (eds.), *Op. cit.*, p. 54

סיכום

בסופו של דבר, ארגון מרחב הסייבר הוא במידה רבה תמונת מראה לארגון החברה במרחב הפיזי. באופן כללי, אפשר לתאר את הארגון הזה באופן הבא: במרחב הסייבר פועלים גורמים פרטיים לצד גורמים מדינתיים (בניהם הצבא). על כל אחד מגורמים אלה מוטלת החובה לאבטח את עצמו ואת מערכתיו. גופי המדינה ולעיתים גם גופים פרטיים נבחרים (כגון תשתיות חיוניות במדינות מסוימות) מוגנים או על ידי סוכנות ייעודית, או על ידי הסוכנות האחראית על ביטחון הפנים ואילו רדיפת פושעים ותפיסתם מוטלת על גורמי אכיפת החוק. הצבא, מצידו, מגן על מערכתיו ותוקף גורמים תוקפניים – לרוב כאלה הממוקמים פיזית מחוץ למדינה.

בהינתן סכימה כללית זו, אפשר לראות שרוב השאלות המהותיות הקיימות נוגעות לא בהכרח לארגון מרחב הסייבר ולפעולה בו, אלא לתפקידי הגורמים השונים בתוך המבנה החברתי הזה ובמיוחד לסוגיית השיתוף במידע וגבולות הגזרה הספציפיים בין האזרחי לממשלתי **בתוך המדינה**. סביר שגם סוגיות אלה יוסדרו בסופו של דבר באופן העומד בקנה אחד עם ערכי החברה הכלליים ועם הארגון החברתי הנהוג בה – לדוגמה, במדינות דמוקרטיות יקבע שהמדינה אינה יכולה לרגל אחרי אזרחיה ברשת ללא אישור מערכת המשפט, אך מותר לה לרגל אחרי אזרחים זרים (בכפוף לאישור הדרג המדיני וכו'). לשם כך, נדרשת הסדרה בעיקר בתחום החקיקה, התקנון והמדיניות ונראה שזה עיקר תפקידה המדינה (כמדינה).

בהתאם, יש לשער שנקודות תורפה משמעותיות יהיו קווי התפר בין גבולות הגזרה – כשם שקורה תדיר במרחבים הפיזיים. בהקשר הביטחוני, סוגיה משמעותית תהיה ההתמודדות עם איומים "הברידיים" הכוללים הן מימד טרור, הן מימד פלילי והן מימד מדינתי. איומים אלה יצריכו – שוב, כמו מקביליהם במרחב הפיזי – מאמץ רב-סוכנותי.

קו מאמצים משמעותי בכל הנוגע לפעולה במרחב הסייבר הוא שיתוף המידע. כיוון שליבת המרחב היא מידע וכל המתרחש בו הוא מעבר של מידע ונתונים, לשיתוף במידע ערך ניכר – הן למדינה והן לגורמים פרטיים. כך, אפשר שעיקר הסיוע של המדינה לגורמים במגזר הפרטי תהיה שיתוף במידע על איומים ובמודיעין רלוונטי, אותו היא משיגה באמצעות מגוון ארגוני המודיעין שלה (הן באמצעות מרחב הסייבר והן מחוצה לו). הסוגיות והאתגרים הנוגעים בשיתוף המידע הנוגע במרחב הסייבר דומים ביסודם לאלה הנוגעים במרחבים אחרים – מה יש לשתף, כיצד לשתף מבלי לחשוף מקורות וכו'. סוגיות אלה מתחדדות מכיוון שבשונה מהמרחב הפיזי, במרחב הסייבר נדרשת המדינה לחשוף מידע רב בפני גורמים פרטיים, ללא סיווג ביטחוני מתאים ולעיתים אף עם קשרים נרחבים עם מדינות זרות. לפיכך, מדובר בסוגיה

משמעותית המחייבת הסדרה עקרונית – על אחת כמה וכמה בהינתן אתגרי שיתוף המידע שלעיתים קיימים כבר היום בקרב סוכנויות המודיעין השונות.

סוגיה נוספת הרלוונטית לפעולת המדינה במרחב הסייבר היא סוגיית הכשרת כוח אדם והסדרת הידע הטכני של העוסקים בתחום – בעיקר בהיבטי איכות כוח האדם ולא בהיבטי התכנים. זאת בדומה למקצועות חשובים אחרים - כגון רופאים, אדריכלים, עורכי דין וכו' – או תחומי ידע אחרים שנחשבים לנדרשים על ידי המדינה (כגון, בעבר, ידיעת השפה הערבית). כיום מקובל להגיד שהמשאב היקר ביותר בכל הנוגע למרחב הסייבר הוא ההון האנושי. לשם ניהול מבצעים במרחב הסייבר, נדרשת המדינה להיות מסוגלת "לייצר" מקצועני סייבר באופן "תעשייתי", כשם שהיא מייצרת כוח אדם צבאי מעולה אחר כגון טייסים או אנשי כוחות מיוחדים ובהיקפים דומים. קו המאמצים של הכשרת כוח האדם הוא חלק ממלאכת בניין כוחות הסייבר של המדינה באופן כללי ולא רק של הצבא. זאת כיוון שמדובר במלאכה המצריכה מגוון שינויים ארגוניים וחקיקתיים בסוכנויות המדינה השונות העוסקות בתחום. סביר שכל שיתבגרו הדורות של אנשים שהם "ילידים דיגיטליים" (Digital Natives) יגדל מאגר כוח האדם הזמין לגיוס למערכי הסייבר, עם זאת, אל למדינה להניח לתהליכים אלה "להתנהל מעצמם". כשם שהמדינה אינה מסוגלת להסתפק באנשים שיודעים לטוס כפועל יוצא מהכשרה עצמית לשם איוש חיל האוויר, כך אל לה להסתמך בעיקר על אנשים כגון אלה לאיוש כוחותיה למבצעים בסייבר. שיפור הכשרת הסייבר הוא אחד מתחומי האחריות העיקריים של המדינה וזה שעשוי להניב את התשואות הגבוהות ביותר.

בקו מאמצי ההכשרה אפשר לכלול גם את אחריות המדינה לשיפור מיומנות האזרחים להתגונן במרחב הסייבר. אם מרחב הסייבר הוא מרחב ככל המרחבים הפיזיים האחרים, הרי שהכשרת האזרח לפעולה במרחב זה נמצאת גם היא באחריותה של המדינה, כשם שהקניית מיומנויות בתחום הזהירות בדרכים היא באחריות המדינה. האינטרס של המדינה לדאוג לכך, מעבר לחובתה לדאוג לטובת האזרח, היא שאזרחים מיומנים יותר בשימוש במרחב הסייבר ובהתגוננות בו ישפרו את ביטחון המרכיבים האחרים "מלמטה למעלה". אי לכך, נדרשת היערכות של המדינה להקנות מיומנויות "תקשוביות" מגילאים צעירים ואף צעירים מאוד.

סוגיה נוספת הנדרשת להסדרה היא האופי הרב לאומי של חלק מהגורמים הפועלים במרחב הסייבר. כך לדוגמה, נשאלת השאלה מה בדבר ההשפעות עקיפות על ישראל של התקפות על מטרות אחרות – לדוגמה, השפעה על ישראל של התקפה של גורם שלישי על חוות שרתים מרכזית של גוגל כחלק מהתקפה על ארה"ב או על מדינה אחרת במרחב? מכיוון שבשונה מהמרחב הפיזי, לפעולות במרחב הסייבר יש השפעות חוצות גבולות, נדרשת הסדרה של הגורמים המטפלים בסוגיות כאלה ושל סמכויותיהם, כמו גם של הנהלים בעת האירוע, לפניו

ואחריו. אפשר שבמקרה זה יוסדרו הסמכויות וגבולות הגזרה בדומה למקבילים במרחב הפיזי – כך, המשטרה תעסוק באיומי פשיעה רב-לאומיים והשפעותיהם, הצבא ושירותי הביון יעסקו באיומי טרור והתקפה מצד גורמים מדינתיים וכו'.

כך או כך, לא נראה שיש חולק על הקביעה שהמגזר הפרטי הוא הגורם החזק והמוביל במרחב הסייבר והוא נדרש להגן על עצמו בעצמו. עם זאת, נדרשת חשיבה על האתגרים של העסקים הקטנים החשופים לפגיעות במרחב הסייבר ובתוך כך מסכנים הן את עצמם והן ארגונים גדולים יותר הנמצאים עימם בקשר. נדרשת חשיבה כיצד יכולה המדינה לשפר את איתנותם של גורמים אלה במרחב הסייבר מתוך ההבנה שרוב הפריצות במרחב זה מתגלות על ידי גורם שלישי (בשונה מהמתרחש במרחב הפיזי), אך שגורמים המסוגלים לגלות את פרצותיהם בעצמם, מסוגלים להכיל פרצות אלה מהר יותר. סוגיית התמודדות העסקים הקטנים (והבינוניים) עם פגיעות במרחב הסייבר היא אולי הסוגיה המשמעותית ביותר המונחת לפתחה של המדינה (לבד מסוגיית הפגיעות של התשתיות הלאומיות החיוניות) - הן מכיוון שעסקים אלה פגיעים הרבה יותר מתשתיות לאומיות¹³³ והן מכיוון שפגיעה נרחבת בעסקים קטנים ובינוניים עשויה לפגוע ישירות, במהירות ובמידה בולטת מאוד ב"אזרח הקטן". כיוון שעסקים אלה לא מסוגלים להגן על עצמם במחיר שניתן לעמוד בו (בשונה מאשר במרחב הפיזי), כאן הוא המקום לפתרונות יצירתיים וחדשניים על ידי המדינה או בעידודה (הישיר או העקיף).

כיוון שגורמי איום שונים נוטים לתקוף מטרות שונות, אפשר להסיק שהאיום על המגזר הפרטי שונה מאשר האיום על המגזר הציבורי ועל התשתיות החיוניות ושונה מאוד מהאיום על המערכות הצבאיות. בהינתן שוני זה, נשאלת השאלה מה תפקיד הממשלה בפעולה כנגד האיומים השונים ואילו סוכנויות נדרשות לטפל בכל איום? בהתאם, אפשר שהסיוע של המדינה ומידת האחריות שלה יהיו מותאמים "ללקוח". כך, המדינה תסתפק ברגולציה על שחקנים גדולים ולא חשופים ורבי השפעה ובד בבד תנסה לעודד, לידע ולסייע באופן פעיל יותר לשחקנים קטנים יותר ומשפיעים פחות (או להפך). בהתאם, אפשר להקביל את המאבק בפשיעת הסייבר למאבק בפשיעה הרגילה. לדוגמה, כאשר נאבקים במבריחי נשק, עושה זו המשטרה, בסיוע מודיעיני של שירותי הביטחון האחרים והצבא. אולם, כאשר מבריחי נשק אלה הם טרוריסטים, נאבקים בהם שירותי הביטחון השונים או הצבא.

כיוון שלציבור כולו עניין במרחב הסייבר וכיוון שמרחב זה הוא ציבורי ופרטי ברובו, הסדרת אבטחתו וההתנהלות בו תחייב דיון ציבורי פתוח, המלווה בהסברה בנוגע לאתגרים הקיימים

¹³³ הן עקב גודל החברות המטפלות בתשתיות אלה ויכולתן לעמוד בהוצאות הכרוכות בהקמת אגפי אבטחה במרחב הסייבר והן עקב העובדה שפגיעה בתשתיות פיזיות (Operational Technology) – ולעיתים קרובות אנלוגיות – היא משימה מורכבת הרבה יותר מאשר פגיעה בטכנולוגיות מידע (Information Technology).

ולנקודות הפגיעות הטבועות במרחב ובטכנולוגיה. "תיאום ציפיות" זה עם הציבור הרחב ועם המגזר הפרטי הוא בראש ובראשונה באחריות המדינה. האופי החשאי והטכני עד מאוד של הדין הנוכחי במרחב הסייבר לא תורם להבנה הציבורית של המרחב ולהסדרת ההתנהלות בו (ואולי אף מחבל בהם). אפשר שהעברת חלק מסמכויות ההגנה במרחב הסייבר לגורמים "גלויים", כגון המשטרה ועיסוק הולך וגדל בגורמי "רכים" יותר הנמצאים בסמכות המדינה (כגון חינוך והכשרה), יתרמו לפתיחת הדין לציבור.

כל הנושאים האלה הם בראש ובראשונה נושאים של הסדרת סמכויות. לא מדובר על נושאים בינאריים להם מענה החלטי זה או אחר. כמו כן, לא מדובר על סוגיות שאפשר להותיר לפתחה של "המערכת" ופקידיה או להתנהלות מכוח האינרציה. מרחב הסייבר הוא מרחב חדש וככזה, יש בהסדרתו המודעת פוטנציאל להימנע מנפילה למכשלות ארגוניות ישנות או לבעיות קיימות. אך ההסדרה המודעת של מרחב הסייבר מחייבת החלטות ברורות ועקרוניות. אי אפשר להתיר את הסוגיות השונות לטיפולם של ארגונים קיימים רק בגלל שהם כבר קיימים. יש לדון בכך ולהסדיר את הסוגיות השונות מתוך הבנה הן של הצרכים הייחודיים של מרחב הסייבר והן של ההשפעה של סמכויות חדשות במרחבים חדשים על הן הארגונים הקיימים והן על פעילויותיהם במרחב החדש.

ההחלטות העקרוניות האמורות נדרשות להתקבל בדרגות הגבוהות ולהתבטא במסמכי האסטרטגיה והתפיסה הבסיסיים. כפי שטוענת תפיסת הסייבר של משרד ההגנה האמריקני, כדי להתמודד עם התקפות במרחב הסייבר, נדרשת אסטרטגיה כוללנית ומקיפה.¹³⁴ בהתאם, תפיסת הסייבר הבסיסית של המדינה נדרשת להגדיר את עקרונות הפעולה של המדינה במרחב הסייבר בכל התחומים העיקריים ולא רק בתחום הביטחוני. לכן, טעות תהיה למקד את הדין אך ורק במישור הביטחוני (או הצבאי) ולערוך את הדין אך ורק בקרב יודעי ח"ן. הדין הבסיסי במרחב הסייבר נדרש להיות פתוח ולערב מגוון גורמים, הן מהמגזר הממשלתי והן מהמגזר הפרטי. על בסיס דיון זה – ומסמכי התפיסה הבסיסיים שייכתבו כפועל יוצא ממנו – יש לערוך את הדיונים הביטחוניים המסווגים ולא להיפך.

¹³⁴ The Department of Defense Cyber Strategy, p.2

שמור

נספח א' – שאלות למחקרים נוספים

במהלך העבודה על מחקר זה, עלו מספר סוגיות שאפשר לטפל בהם במסגרת מחקרים עתידיים. שאלות אלה הן כדלהלן:

ההתקפה בסייבר

- מה מקום ההתקפה במרחב הסייבר?
- האם אפשרית¹³⁵ התקפת מנע או התקפת ענישה (בהגיון הרתעתי\הגנתי) במרחב הסייבר, האם היא נדרשת ואילו צעדים צריכה המדינה לבצע כדי לאפשר זאת?
- מי מוסמך להפעיל אלימות במרחב הסייבר?

האיומים הטקטיים במרחב הסייבר

- מה הם האיומים ה"קטנים" טקטיים במרחב הסייבר¹³⁶ ומה היא השפעתם האפשרית??

מקבילות היסטוריות למרחב הסייבר

- האם קיימים דגמים מקבילים – היסטוריים¹³⁷ או נוכחיים – שיקלו על הסדר פעולת המדינה במרחב הסייבר?

המדינה והמגזר הפרטי

- מה גבולות אחריות המדינה כלפי המגזר הפרטי ומה הן סמכויותיה ביחס אליו?
- מה היא אחריות המדינה כלפי העסקים הזעירים והאזרחים היחידים בכל הנוגע לאבטחת מרחב הסייבר?
- כיצד יכולה המדינה לסייע לגורמי המגזר הפרטי בכל הנוגע לאבטחת מרחב הסייבר וכיצד יכולים גורמי המגזר הפרטי לסייע למדינה במשימה זו?

אחרות וסמכות במרחב הסייבר

- מה הן סמכויות גופי הביטחון השונים בכל הנוגע למרחב הסייבר?

הרתעה במרחב הסייבר

¹³⁵ מבחינה חוקית ותפיסתית.

¹³⁶ לדוגמה – מערכת טרור כלפי אזרחים ועסקים קטנים, מקבילה במידה זו או אחרת לטרור הסכינאות הקיים כיום.

¹³⁷ לדוגמה – פעולת המדינה בימים במאות ה-17 וה-18, פעולת המדינה בחלל החיצון, פעולת המדינה באמצעות שכירי חרב וכו'.

שמור

- האם ישנם דגמי הרתעה מוצלחים במרחב הסייבר וכיצד אפשר להשיג הרתעה במרחב זה?

ביבליוגרפיה:

יוסי הוכבאום, "המרחב הקיברנטי – הגדרתו, קווים לתפיסת המבצעים במרחב וארגון הפיקוד על ניהולם על פי המודל האמריקני", בתוך: אמ"ץ-תוה"ד, **המרחב הקיברנטי (הסייבר)**, תצפית 61, אפריל 2011, ע"מ 66-7

שמואל אבן, "אסטרטגיה לשילוב המגזר הפרטי בהגנת הסייבר הלאומי בישראל", **צבא ואסטרטגיה**, כרך 7, גליון 2, INSS, ספטמבר 2015

Adam Segal, "America is Learning the Hard Way How To Respond to Cyber Threats", **Defense One**, 18 Dec. 2014

Ashton B. Carter, "Rewriting the Pentagon: Charting a New Path on Innovation and Cybersecurity", **Defense.gov**, 23 Apr. 2015, www.defense.gov/News/Speeches/Speech-View/Article/606666/drell-lecture-rewriting-the-pentagon-charting-a-new-path-on-innovation-and-cyber

David Burg et. al., **US Cybersecurity: Progress Stalled – Key Findings from the 2015 US State of Cybercrime Survey**, PwC, July 2015

David Chismon and Martyn Ruks, **Threat Intelligence: Collecting, Analyzing, Evaluating**, CPNI: MWR Infosec, 2015

David Clarck, Thomas Berson and Herbert S. Lin (eds.), **At the Nexus of Cybersecurity and Public Policy – Some Basic Concepts and Issues**, Washington, DC: National Academies Press, 2014

Daniel Manson and Ronald Pike, "The Case for Depth in Cybersecurity Education", **ACM Inroads**, Vol. 5, No. 1, March 2014

Dustin Volz, "FBI Director: Encryption Is Great As Long As It Lets Us In", **Defense One**, 6 Jul. 2015, www.defenseone.com/technology/2015/07/fbi-director-encryption-great-long-it-lrts-us/116998/

Elias Groll, "Controversial Cybersecurity Measures Set for Final Approval", **Foreign Policy**, Dec. 16 2015,

www.foreignpolicy.com/2015/12/16/controversial-cybersecurity-measure-set-for-final-approval

Garance Burke and Jonathan Fahey, "AP Investigation: US Power Grid Vulnerable to Foreign Hacks", **ABC News**, 21 Dec. 2015, www.abcnews.go.com/US/wireStory/ap-investigation-us-power0grid-vulnerable-foreign-hacks-35882487

Gregory Conti and John "Buck" Surdu, "Army, Navy, Air Force and Cyber – Is It Time for a Cyberwarfare Branch of Military?", **IAnewsletter**, Vol. 12, No. 1, Spring 2009

High Representative of the European Union for Foreign Affairs and Security Policy, **Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace**, Brussels: European Commission, Feb. 2 2013

Isac R. Porche, "Cyberwarfare Goes Wireless", **RAND**, Apr. 4 2014, www.rand.org/blog/2014/04/cyberwarfare-goes-wireless.html

James A. Lewis, **Raising the Bar for Cybersecurity**, Center for Strategic and International Studies, 12 Feb. 2013

Jason Healey, **Breaking the Cyber-Sharing Logjam**, Atlantic Council, Feb. 2015

Lilian Ablon, **Lessons from a Hacker: Cyber Concept for Policymakers**, RAND, Sept. 14 2015, www.rand.org/multimedia/video/2015/09/14/lessons-from-a-hacker-cyber-concepts-for-policymakers

Loren Thompson, "Five Reasons Why Silicon Valley Won't Partner With the Pentagon", **Forbs**, 27 Apr. 2015, www.forbs.com/sites/lorenthompson/2015/04/27/five-reasons-why-silicon-valley-wont-partner-with-the-pentagon/

Martin C. Libicki, "Don't Buy the Cyberhype", **Foreign Affairs**, Aug. 14, 2013, www.foreginaffairs.com/articles/united-states/2013-08-14/dont-buy-cyberhype

Mandiant 2013 Threat Report - **M-Trend: Attack the Security Gap**

Michael Casey and Robert Hackett, "The Biggest R&D Spenders Worldwide", **Fortune**, 17 Nov. 2014, www.fortune.com/2014/11/17/top-10-research-development/; Brad Reed, "Samsung is Spending an Insane Amount of Money to Beat Apple to the 'Next Big Thing'", **BGR**, 10 Mar. 2015, www.bgr.com/2015/03/10/samsung-r-and-d-spending-2014/

National Cybersecurity and Communications Integration Center, www.dhs.gov/national-cybersecurity-communication-integration-center

P. W. Singer, "How the United States Can Win the Cyberwar of the Future", **Foreign Policy**, 18 Dec. 2015, www.foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/

Peter Bright, "Report: NSA Paid RSA to Make Flawed Crypto Algorithm the Default", **Ars Technica**, 21 Dec. 2013, www.arstechnica.com/security/2013/12/report-nsa-paid-rsa-to-make-flawed-crypto-algorithm-the-default/

Peter Bright, "The NSA's Work to Make Crypto Worse and Better", **Ars Technica**, 6 Spe. 2013, www.arstechnica.com/security/2013/09/the-nsas-work-to-make-crypto-worse-and-better/

Pierre Blenaine, "This Chart Shows How The US Military Is Responsible for Almost All the Technology in your iPhone", **Business Insider**, 29 Oct. 2014, www.businessinsider.com/the-us-military-is-responsible-for-almost-all-the-technology-in-your-iphone-2014-10

Privacy Impact Assessment Einstein Program – Collecting, Analyzing and Sharing Computer Security Information across the Federal Civilian Government, Washington, DC: Department of Homeland Security, National Cyber Security Division – Computer Emergency Readiness Team

Richard J. Danzig, **Surviving on a Diet of Poisoned Fruit – Reducing National Security Risks of America's Cyber Dependencies**, Center for a New American Security, July 2014

Trustwave Global Security Report 2015

The Department of Defense Cyber Strategy, Washington, DC: Department of Defense, 17 Apr. 2015