יתרון שאינו רק טכנולוגי – השינוי הארגוני בארצות הברית בתחום הלוחמה במרחב הסייבר

עמית שיניאק

מרוץ החימוש בתחום הסייבר הוא חלק מהמציאות הביטחונית המדינתית בימינו. מאמר זה מעלה את הטענה כי מאפייניו הייחודיים של ממד הסייבר והירידה ברמת התחכום הטכנולוגי הנדרשת למימוש יכולות תקיפה והגנה בו, גורמים לכך שהשגת יתרון ביטחוני בממד זה מחייבת קידום ופיתוח יצירתיים בתחום ארגון הכוח וגיבוש תורת לחימה צבאית המשלבת בין הפעילות הביטחונית במרחב הסייבר הווירטואלי ובין מרחבים פיזיים. טענת המאמר מתבססת על סקירה מקיפה של החקיקה, התוכניות וההחלטות סביב תהליך בניין הכוח, הארגון ותורת הלחימה של מבצעי סייבר בארצות הברית, מראשית שנות השמונים של המאה העשרים ועד שנת 2012. המאמר מדגיש את השינויים והעלייה בהיקף האיומים במרחב הסייבר, את השינויים בתפיסת האיום ואת המעבר מגישה טכנית לגישה הרואה באינטרנט מרחב לחימה בעל מאפיינים ייחודיים. מסקנותיו של המאמר רלוונטיות לאנשי מקצוע ומקבלי החלטות כאחד ומכוונות להביא לארגון ופיתוח תורת לחימה בצבאות ובארגוני ביטחון אזרחיים כצעד הכרחי בדרך ליצירת יתרון אסטרטגי במרחב לחימה זה. למרות שהמאמר מתמקד בארצות הברית ובפרק זמן מוגבל בלבד, משרתו היא להפנות זרקור לתחום הארגון כזירה רלוונטית ומשמעותית להשגת יתרון מדיני בתחום ביטחון הסייבר, וזאת מול המצב השורר כיום, בו קיימת התמקדות יתר בקרב חוקרים ומקבלי החלטות בפיתוח טכנולוגי ככלי המרכזי להשגת יתרון בתחום זה.

מילות מפתח: מרחב הסייבר, ביטחון סייבר, בניין כוח, ארגון, תורת לחימה, ארצות הברית, יתרון אסטרטגי, דומיננטיות.

ד"ר עמית שיניאק הוא עמית מחקר פוסט־דוקטורנט בתוכנית ללימודי מדע, טכנולוגיה וחברה (STS) בבית הספר קנדי לממשל באוניברסיטת הרווארד.

מבוא

המאבק הבין־מדינתי בתחום הסייבר הוא עובדה ידועה זה מכבר ונושא שכיח למחקרים בתחום הביטחון והיחסים הבין־לאומיים.[1] מרוץ החימוש ובניין הכוח הצבאי בתחום הסייבר מוצאים את ביטוים בעלייה המשמעותית בהקצאת משאבים לאומיים ליצירת ביטחון במרחב זה.[2] לאור פעילות אינטנסיבית זו, ראוי לשאול מה היא הדרך להשיג יתרון מדינתי במרוץ החימוש הקיים בתחום הסייבר?

במאמר זה אטען כי החזית במרוץ החימוש הקיברנטי נמצאת לא רק בפיתוח טכנולוגי של כלי פעולה חדשים ומתקדמים יותר ובהשגת ניסיון מבצעי במרחב הסייבר, אלא גם, ובמיוחד, בהתקדמות בארגון כוחות הביטחון ויחידות הצבא הפועלים במרחב זה ובתיאום בין הדרגים המדיני והצבאי. זאת, באופן שיבטא שינוי בתפיסת האיום של מרחב הסייבר על מדינות ובדרך הפעולה הצבאית הנדרשת כדי להתמודד איתו. במילים אחרות, למרות שאנו חיים בתקופה שבה ניתן לפתח יכולות לוחמת סייבר בקלות יחסית, ורמת התחכום הנדרשת מהתוקף נמצאת בירידה, המאבק בין מדינות באמצעות מרחב הסייבר מחייב חשיבה שונה: השקעה בתהליכי ארגון ובניין כוח עשויה להיות הגורם המבדיל בין מדינות בעלות דומיננטיות בתחום הסייבר ובין שחקנים בין־לאומיים אחרים, ולכן, כדי להשיג יתרון מדיני במרחב הסייבר היא עדיפה על השקעה בפיתוח טכנולוגי.[3]

המאמר אינו מציג מחקר השוואתי,[4] אך הדוגמה האמריקאית שתפורט בהרחבה בהמשך הינה משמעותית, משום שהיא מעידה על שינוי תפיסתי וארגוני, במסגרתו

---

1 ראו כמה דוגמאות ידועות לכך: Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington: CCSA Publication, 2013); Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2007); Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2009); Ben Buchanan, *The Cybersecurity Dilemma: Hacking Trust and Fears between Nations* (New York: Oxford University Press, 2016); P. W. Singer and Allen Friedman, *Cybersecurity and Cyberwar: What everyone Needs to Know* (Oxford: Oxford University Press, 2014); Harris Shane, *@War: The Rise of the Military-Internet Complex* (New York: Mariner Books, an Eamon Dolan Book, 2015).

2 ניתן לראות זאת בנתונים של חברות ביטוח בין־לאומיות, למשל:
"Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Future", *Atlantic Council and Zurich Insurance Group Report*, September 10, 2015, Figure 13, http://publications.atlanticcouncil.org/cyberrisks//.

3 המונח "ארגון ובניין הכוח" מכוון לתהליך התכנון, השינוי והסדרת האחריות בין גופים שונים על תחום לחימה מסוים, וזאת לצורך שליטה, בקרה, פיתוח כוח אדם, אמצעי לחימה ודוקטרינה ייעודיים.

4 להשוואה בין ארצות הברית, ישראל וסין ראו: עמית שיניאק, **המרחב המקוון כאזור גבול: תהליך יצירת הריבונות ויכולת האכיפה במרחב המקוון בישראל, ארה"ב וסין**, הוצאת המחבר, ירושלים, 2015.

אימצה ארצות הברית גישה הרואה בסייבר "מרחב סייבר" ("Cyberspace"), או באופן מדויק יותר "מרחב לחימה".[5] זהו הבסיס לתפיסה הצבאית בארצות הברית היום, שממנו נובע ארגון הכוח האמריקאי בתחום הסייבר, המתבסס על גישה הרואה, כאמור, בסייבר מרחב לחימה. מרחב לחימה זה מצריך פעולה מדינית וצבאית משולבת, בדומה לפעולה הנדרשת לשימור הביטחון הטריטוריאלי והאינטרסים של המדינה במרחבים הפיזיים – באוויר, בים וביבשה.[6]

טענה זו תיבחן במאמר באמצעות ניתוח התפתחות התפיסה הביטחונית, ובמיוחד ארגון ובניין הכוח בתחום הסייבר בארצות הברית, כפי שהדבר מתבטא במסמכים רשמיים גלויים. זאת, בחלוקה לשלוש תקופות: בין השנים 1983–1998, שבהן חל תהליך של הפנמת הסיכונים הפוטנציאליים הגלומים בסייבר לאינטרסים מדיניים והחל תהליך ארגון ביחידות המודיעין האמריקאיות בניסיון לאבטח את המידע הקיים במערכות התקשורת החשאיות מתָווכות המחשב; בין השנים 1998–2008, במהלכן הופנמו במסד הביטחוני האמריקאי המשמעויות של קיומן התקין של מערכות תקשורת מתָווכת מחשב והשלכותיהן על תפקודם הסדיר של תשתיות בסיס ומשאבי יסוד הנדרשים לקיומה של מדינה מודרנית (כגון: מים ומזון, אנרגיה ותחבורה); בין השנים 2008–2012, בהן התרחש מהפך בתפיסת מרחב הסייבר, שבמסגרתו אומצה גישה הרואה במאמץ הצבאי במרחב זה מאמץ מקביל ומשיק לממדים הנוספים (ים, אוויר, יבשה).

הסקירה שתוצג במאמר זה מראה כי ההיגיון המנחה את בניין הכוח לפעולה במרחב הסייבר בקרב מדינות ומעצמות כמו ארצות הברית עבר תמורות לאורך שלושים השנים האחרונות, וזאת לאור העלייה באיום הסייבר ובהשפעתו על מגוון של אינטרסים מדינתיים. תמורות אלו תומכות בטענת המאמר כי ארצות הברית, כמעצמה בתחום הסייבר, היא גורם מוביל בתחום זה גם משום שהיא ארגנה מחדש את כוח הסייבר הצבאי שלה על בסיס אותו היגיון שהנחה אותה בארגון כוחותיה הצבאיים במרחבי הים, האוויר והיבשה. אין בכוונת המאמר לנתח את המחלוקות באשר ליתרונות ולחסרונות של מאפייני ארגון הכוח בתחום הסייבר בתוך הצבא,[7] או ליישב ביניהן. כוונתו היא להדגיש את החשיבות שבקידומו של ארגון הכוח במרחב הסייבר ושל תפיסת הפעלתו, וכן את חשיבות הצורך להתארגן סביב

5 גישה זו באה לידי ביטוי גם בשינוי בהגדרת המונחים המקצועיים המתייחסים אל הסייבר היום כסביבה/ממד/מרחב.

6 יש לציין כי כמה מחקרים העוסקים בשימוש בשפה, במטאפורות, בדימויים ובמודלים מתחומי ביטחון וטכנולוגיות אחרים, במיוחד נשק גרעיני, גם מתייחסים לחשיבות השינוי התפיסתי בתחום ביטחון הסייבר, אך אינם מדגישים את השינוי הארגוני המוסדי עליו מרחיב מאמר זה.

7 למשל, בשאלה האם יש לשלב את גורמי ההגנה, ההתקפה ואיסוף המודיעין באותו גוף, האם לשמר את הדומיננטיות של גורמי המודיעין או הטכנולוגיה, וכדומה.

הרעיון שהסייבר הוא מרחב לחימה מקביל למרחבי לחימה פיזיים. זאת, לעומת התפיסה הרווחת היום בקרב אלה החוקרים את תחום הביטחון בסייבר, הממקדת את תשומת הלב של מקבלי ההחלטות והחוקרים בפיתוח הטכנולוגי ובניסיון המבצעי ככלים המרכזיים וכמוקדי השקעה עיקריים להשגת יתרון בתחום זה.[8]

ניתן להרחיב ולטעון כי תפיסה זו של מרחב הסייבר היא המבדילה בין פעולה צבאית של מדינות מובילות בתחום ביטחון הסייבר (כגון ארצות הברית) ובין ישויות פוליטיות ושחקנים מדינתיים, על־מדינתיים ותת־מדינתיים אחרים. הראשונות מפעילות מאמץ צבאי סדור ומתואם הנשען על תוכניות ופקודות רשמיות שמטרתן להגשים תכלית טקטית ו/או אסטרטגית מסוימת במרחב הסייבר (בדומה לפעולות בים, באוויר וביבשה). האחרונות פועלות במרחב הסייבר בצורה שאינה סדורה, אלא בעלת דפוס רשתי ו"טפילי", הדומה יותר לפעולות טרור או ללחימת גרילה, כגון חבלה, שיבוש, הפחדה והשפעה על התודעה, שנעשות באמצעות תקשורת ממוחשבת.

1983–1998: תפיסת אבטחת המידע

בתקופה שבין שנת 1983, בה הופרדה מערכת המחשבים הצבאית האמריקאית (Milnet) מרשת המחשבים האזרחית, ובין השינוי במאפייני האיום ב־1998 התחולל שינוי משמעותי בתפיסת האיום בתחום אבטחת המידע מתָווך המחשב (ICT), ובהתאם לכך בארגון ובבניין הכוח הביטחוני האמריקאי באותו תחום. עיקרו של השינוי נבע מגישה אמביוולנטית יותר כלפי היתרונות והחסרונות שבתקשורת מתָווכת מחשב. הדבר התבטא במעבר מפעולות מדינתיות שיועדו בעיקרן לשפר ולייעל את זרימת המידע לצורך קידום פעילות אזרחית מחקרית וכלכלית, לפעולות שמטרתן ליצור בקרה, שליטה וחסמים כדי להגן על מידע מדיני רגיש (ביטחוני ואזרחי) שנתפס כמאוים בשל אותה זרימת מידע.

המשמעויות המעשיות של בניין הכוח של ארצות הברית במרחב הסייבר באותה העת התבטאו בעיקר בפעולות להגנת ואבטחת מידע רגיש, באופן שניתן לתאר אותו כיישום או הרחבה של תפיסת ההגנה על המידע, כפי שהייתה קיימת אז בקרב צבאות וארגוני ביון, על מאגרי המידע הממוחשבים שהפכו עם השנים לאמצעי עיקרי לשימור וניהול מידע זה. לפיכך, הפעולות העיקריות שננקטו ביחס לרשתות המחשבים של ארגוני המודיעין והצבא כוונו לשיפור היכולת לשלוט במידע חשאי ומסווג (יצירת רשת תקשורת מחשבים נפרדת וסגורה לצבא היא דוגמה ברורה לכך), ולראשונה גם להשגת מידע חשאי ובעל ערך במסגרת לוחמת

8 ראו, למשל, את הנטייה לניתוח טכנולוגי בכתבי העת *The Cybersecurity Journal, The Journal of Cyber Policy* ודומיהם, המדגישים את הפיתוח הטכנולוגי והניסיון המבצעי ככלים מרכזיים להערכת הביטחון בסייבר ולקידומו.

מודיעין ומידע ולגיבוש הסמכות המדינית המשפטית הנדרשת לשם כך. בתקופה זו הוקמו מוסדות ויחידות ייעודיות, שונו הגדרות האחריות של גופי ממשל וביטחון קיימים והחלה ראשיתה של חקיקה האוסרת על כניסה לא מאושרת למאגרי מידע ממוחשבים רגישים ומאפשרת ענישה ואכיפה. שינויים אלה לא הובילו, עם זאת, לשינוי משמעותי בחשיבה הצבאית.

עצם יצירתה של הפרדה פיזית ומוסדית בין תקשורת מתֻווכת מחשב צבאית ואזרחית הייתה בעלת משמעות רבה ליצירת יכולת שליטה וביטחון במידע הממוחשב. הפרדה זו נוצרה בעקבות שורת פעולות, שעיקרן הפרדת מערכת התקשורת הצבאית ממערכת התקשורת האזרחית בשנת 1983; יצירת מערכת סיווג המאפשרת רק לבעלי תפקידים רלוונטיים לפעול בה;[9] וחקיקה מ־1984 שאסרה על כניסה ללא רשות של אזרחים למערכות מחשב פדרליות שהוגדרו כ"מערכות מחשב מוגנות"[10]("Protected Computers") והרחיבה את סמכות השירות החשאי האמריקאי להגן עליהן.[11]

פרסומים על פרשיות ריגול ופשיעה באמצעות פריצה למערכות מחשב, למשל פרשיית "ביצת הקוקייה"[12]("The Cucko's Egg") ומעצר כנופיית "414" בשנת 1983, הובילו לחקיקה נוספת בשם "Computer Security Act of 1987",[13] שחייבה פיתוח קריטריונים ותקנים לאבטחת מידע ממוחשב ברשויות הפדרליות האמריקאיות,[14] הכשרת כוח אדם ייעודי ומתן הדרכה לעובדים עם מערכות מחשב בדבר הסכנות הפוטנציאליות.[15] בנוסף לכך נקבע באותו חוק כי המערכת הביורוקרטית האזרחית תהיה כפופה בתחום זה לפיקוח והנחייה של סוכנות מודיעין האותות (NSA).[16] הכפפה זו, שהיא אחד מעיקרי השינוי המוסדי שנוצר אז ונאכף עד היום, קיבלה משנה תוקף בהוראה הנשיאותית NSD42 משנת 1990, המנחה לחזק את אבטחת מערכות התקשורת הלאומיות ולבדל אותן ממערכות תקשורת ציבוריות אחרות.[17] הוראה זו מציבה את ראש ה־NSA כסמכות פיקוח בכירה על כלל משרדי הממשלה,

9 תמר אשורי, **מהטלגרף עד המחשב: היסטוריה של אמצעי התקשורת**, רסלינג, תל אביב, 2011, עמ' 138.

10 "18 U.S. Code § 1030: Fraud and related activity in connection with computers", *U.S. Congress*, 1986, §a2C.

11 שם, סעיף D.

12 Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy through a Maze of Computer Espionage* (New York: Doubleday Pocket Books, 1989).

13 "Computer Security Act of 1987", *U.S. Congress*, 1987.

14 שם, סעיף 1.

15 שם.

16 שם, סעיף 5.

17 "National Security Directive No. 42: National Policy for the Security of National Security Telecommunications and Information Systems", *U.S. White House*, 1990, §2.

וזאת באמצעות ועדה בראשות שר ההגנה של ארצות הברית שקמה במסגרת "המועצה לביטחון לאומי".[18]

בשנת 1988, לאור ההד הציבורי שנוצר עקב פעולתו ההרסנית של אחד הווירוסים הראשונים – "תולעת מוריס" ("Morris Worm") – שפגע בכעשרה אחוזים מכלל המחשבים שהיו מחוברים לאינטרנט באותה עת,[19] הוקם ביוזמת המכון להנדסת תוכנה (IES) באוניברסיטת קרנגי מלון, ותחת אחריותו, מרכז הניטור והתגובה הראשון להתמודדות ומזעור נזקים מתקיפות באמצעות מחשבים ("Computer Emergency Response Team" – CERT). למרות שהיוזמה להקמת המרכז הייתה אקדמית, פעל הממשל האמריקאי להחיל ולקבע את פעולותיו כנהוג ביחסי הממשל עם האקדמיה – באמצעות חוזה שקבע כי משרד ההגנה של ארצות הברית יממן את פעולתו, אך גם יגדיר את מסגרת פעולותיו.[20] המרכז שהוקם היווה מאוחר יותר את המודל למסגרות פיקוח וניטור איומים במרחב הסייבר בארצות הברית ובמדינות רבות נוספות.

בתקופה זו רווחה התפיסה הרואה באינטרנט כלי להעצמת יכולת במרחב הפיזי ולאו דווקא מרחב חדש להתנהלות בין מדינות. הדבר עולה מהתפיסה הביטחונית ומהדוקטרינה הצבאית האמריקאית המנוסחות בחזון המטות המשולבים של צבא ארצות הברית שפורסם ב־1996 במטרה לחזות את הדרישות לשדה הקרב העתידי עד שנת 2010. למרות העובדה שהמשמעות של יכולות ממוחשבות כבר הייתה ברורה באותה עת,[21] האינטרנט שהומשג אז לראשונה במסגרת הצבאית כ"רשת המחברת רשתות" ("Network of Networks"), נתפס בעיקר כתשתית בסיסית המאפשרת את היכולת להפעיל אמצעי לחימה מתקדמים המבוססים על רשת נתונים (Information Grid).[22]

זו הייתה הדוקטרינה שהובילה להקמתה, בשנת 1995, של יחידה ייעודית בחיל האוויר האמריקאי ללחימה הגנתית והתקפית באמצעות תקשורת מתֻווכת מחשב, שנקראה The 609th Information Warfare Squadron.[23] לחימה באמצעות

18 שם, סעיפים 4–6.

19 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 26.

20 "U.S. Department of Homeland Security Announces Partnership with Carnegie Mellon's CERT Coordination Center", *SEI Press Release*, September 15, 2003, http://www.sei.cmu.edu/newsitems/uscert.cfm

21 כך, למשל, ההגנה על תשתיות ממוחשבות זכתה להתייחסות במסמך, אך צוינה ככלי שמטרתו העיקרית היא לאפשר עליונות בלוחמת מידע (IW).

22 "Joint Vision 2010", *U.S. Office of the Joint Chiefs of Staff*, 1996, p. 16.

23 היחידה פעלה מ־1995 עד 1999. אז היא הוכפפה לארגון הצבאי החדש בתחום הלחימה בסייבר. להיסטוריה הרשמית של היחידה ראו פרסום של חיל האוויר האמריקאי: "609th IWS: A Brief History, October 1995-June 1999", *U.S. Department of the Air Force*, 1999.

מחשבים עדיין נתפסה אז בקרב הפיקוד העליון האמריקאי כאמצעי לחימה נוסף ולא כמרחב לחימה עצמאי שמתקיימים בו מאמצי הגנה והתקפה,[24] הדורש לכן את ארגון הכוח הצבאי מחדש.[25] גישה זו, שראתה במרחב הסייבר רק אמצעי פרקטי ללחימה (ולא מרחב לחימה חדש), מוצאת ביטוי במזכר רשמי שפרסמו מפקד חיל האוויר ושרת האווירייה האמריקאית בשנת 1997, בו נקבע כי "לוחמת מידע היא אמצעי ולא מטרה, בדיוק כשם שלוחמה אווירית היא אמצעי ולא מטרה בפני עצמה".[26] התפיסה העולה מציטוט זה מעידה על חשיבה צבאית שאינה מזהה את חשיבות המושגים "מרחב" ("Space") או "ממד" ("Dimension") כבסיס לקביעת מדיניות ביטחון בכלל (לא רק באוויר ולא רק בסייבר). ייתכן שגם היום יש בקרב אלה המפעילים אמצעי לחימה במרחב האווירי (וכן הימי והיבשתי) הרואים פעולות בסייבר כאקט תומך בלבד. גישת כותבי המזכר באותה העת הייתה כי איום הסייבר מכוון למידע בלבד והם התקשו לחזות את היקף העיסוק הצבאי בו היום.

1998–2008: תפיסת התשתיות

בתקופה זו חל שינוי משמעותי בתפיסת האיום הנובע מרשתות מחשבים, הן ברמת הדחיפות והן בסיכון שאיום זה מציב לריבונות המדינה וליכולת תפקודה תחת מתקפה. הסיבה לכך הייתה השינוי במאפיינים הטכניים של פריצות למערכות מחשב, שהפכו למורכבות יותר ויותר, בעוד שרמת התחכום והידע הטכני שנדרשה מהפורץ ירדה משמעותית מאז אמצע שנות התשעים של המאה העשרים.[27]

מספר אירועי פריצה למערכות המחשב של הפנטגון בשלהי שנות התשעים, הן במסגרת תרגיל ER97 והן בפרשיית הריגול "Solar Sunrise", נתפסו כ"קריאת השכמה" למערכת הביטחון האמריקאית. הם גם הבהירו כי אין במערכת הצבאית והביטחונית של ארצות הברית גורם אחד המוגדר כאחראי על פעולות נגד איומים מעין אלה.[28] בעקבות זאת התקבלה לראשונה החלטה, בנובמבר 1998, להקים כוח משימה ייעודי – "Joint Task Force for Computer Network Defense" (JTF-

24 ראוי לציין שלמול תפיסה זו של הפיקוד הצבאי העליון רווחה בקרב דרגי העבודה שהקימו את טייסת 609 ההבנה שהם חלוצי הלחימה במרחב חדש. הם אף השוו את עצמם לטייסת הראשונה שפיתחה את תורת הלחימה באוויר ב־1913: שם, עמ' 1.

25 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 31.

26 "Information warfare is a means, not an end, in precisely the same manner that air warfare is a mean, not an end": "Cornerstones of Information Warfare", *U.S Department of the Air Force*, 1997, http://www.c4i.org/cornerstones.html.

27 "Securing the Nation's Critical Cyber Infrastructure", *U.S. Department of Homeland Security*, 2010, p. 3. תשומת לב לגרף בעמוד 3, המצביע על נקודת האיזון בין הדרישות לידע של התוקף ובין רמת התחכום של התקיפה בשנת 1990. בשנת 1995 כבר ניתן היה לרכוש כלי תקיפה מתוחכמים מן המוכן.

28 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 36.

(CND – שהוכפף ל"סוכנות ההגנה למערכות מידע" (Defense Information Systems Agency" – DISA), ומאוחר יותר לפיקוד החלל האמריקאי. כוח המשימה פעל בסנכרון עם ה־NSA ויועד ללחימה במרחב הסייבר ולהתמודדות התקפית (לא פסיבית) עם תקיפות מצד מדינות זרות לצורך אבטחת רשתות מחשב.[29] הכוח, שפורק בשנת 2010, היה גורם משמעותי בקידום המוכנות של ארצות הברית להגנה על מרחב הסייבר, במיוחד בזכות כוח האדם המגוון והרלוונטי שרוכז לצורך הקמת גופים שיוכלו להתמודד עם מבצעי מחשב התקפיים: מומחי מחשבים, אנשי צבא ממגוון זרועות, אנשי מודיעין ואנשי ביטחון. מאוחר יותר אף נשלחו אנשי צבא ללימודים מתקדמים בתחום המחשבים ויצרו שילוב אידיאלי מבחינת הכשרתם המקצועית.[30]

בשנת 2004 קיבל כוח המשימה אחריות על כלל מבצעי ההגנה וההתקפה בתחום הסייבר, ועבר מעיסוק ישיר בתחומים אלה להיות גוף מטה צבאי סדור שאינו פועל בעצמו להגן או לתקוף, אלא מסנכרן ומנחה את כל המפקדות האופרטיביות והיחידות הטקטיות האחראיות על פעולות ביטחוניות במרחב הסייבר בזרועות ובחילות השונים.[31] הגוף החדש – JTF-CNO –הוביל הן לשינוי ביורוקרטי־ארגוני והן לשינוי ביכולת ההתגוננות המעשית של מערכת הביטחון האמריקאית: מבחינה ארגונית, שינוי זה היווה את הפתח להקמתו בהמשך של פיקוד הסייבר; מבחינה מעשית, כוח המשימה, שגובש במקור לצורך התמודדות עם אתגרים ביטחוניים, הפך למשמעותי גם בגיבוש יכולת התמודדות עם סוגיות משיקות, שלא היו חלק מייעודו המקורי אך סיכנו את המוכנות המבצעית ואת הריבונות האמריקאית במרחב הסייבר. מדובר, בין היתר, בווירוסים עצמאיים שתרמו לתחושת האיום בשל ההשלכות האפשריות של פגיעתם בתקשורת מתֻווכת מחשב.

תחושת איום חדשה זו הובילה להגדרת הצורך בהערכת מצב לאומית מתמשכת לאיתור הבעיות הביטחוניות בתקשורת מתֻווכת מחשב, וזאת ככלי לגיבוש מדיניות, לתכנון ולהתמודדות עם בעיות אלו. נקודת התורפה המרכזית שהתגלתה בהערכת המצב הייתה שתשתיות קריטיות ומשאבי היסוד האזרחיים של המדינה, שאינם חסויים ולא חלה עליהם חובת פיקוח והסתרת מידע, פתוחים לפגיעה אפשרית באמצעות תקשורת המחשבים שעליה הם נסמכים. אחד המהלכים להתמודדות עם מִפגע זה היה חקיקתו בשנת 2002 של חוק "Critical Infrastructure Information Act". החוק הגדיר את המונח "מידע תשתיתי קריטי/חיוני" כחלק מתוכנית

29 שם, עמ' 38–40.
30 שם, עמ' 38–39.
31 שם, עמ' 57.

להתמודדות עם פגיעה בתשתית רגישה זו,[32] והרחיב את הגדרת המונח "מערכות מוגנות", כך שתכלול גם מערכות ציבוריות אזרחיות.[33]

בשנת 2003 קיבלו הנשיא בוש הבן והשר להגנת המולדת של ארצות הברית החלטה (Homeland Security Presidential Directive No. 7 – HSPD7) שתיקפה את הצורך בפעילות ביטחונית שאינה צבאית להגנה על תשתיות אזרחיות. הגופים שהוקמו במסגרת זו תחת המשרד להגנת המולדת קיבלו אחריות לניטור, תכנון, הנחייה, הגנה וקביעת עדיפויות במרחב הסייבר (ללא כוחות מבצעיים; אלה נותרו בידי הצבא וסוכנויות המודיעין). כמו כן הואצלו סמכויות למשרדי הממשלה השונים כדי שיקיימו סקר מקיף שיכלול הערכה וסקירה של כלל התשתיות והאינטרסים שבתחום אחריותם, וזאת במטרה לאתר אפשרויות לתקיפת תשתיות על ידי ארגוני טרור באמצעים ממוחשבים.[34] ההחלטה אף יצרה הקבלה בין פגיעה במערכות המחשב של תשתיות מסוימות לבין הפעלת נשק להשמדה המונית.[35] להקבלה זאת הייתה משמעות מבחינה דוקטרינרית, משום שהשתמע ממנה שיש להיערך למניעת איומים ממרחב הסייבר באופן דומה ובהשקעה דומה להיערכות של ארצות הברית אל מול איומים בנשק בלתי קונבנציונלי ואיומים של מתקפות טילים בליסטיים. הקבלה זו גם הובילה את תורת הלחימה בסייבר לשימוש נרחב בדימויים מעידן המלחמה הקרה, כמו "הרתעה" ו"הגנה אקטיבית" – דימויים הרווחים בתחום לוחמת הסייבר עד היום.[36]

התוכנית המדינית שתוכננה לאור סקר המַפגעים פורסמה על ידי ממשל בוש הבן בשנת 2003 וכללה מרכיבים שהצביעו על שינוי תודעתי וארגוני משמעותי הן לגבי הממשל הפדרלי והן לגבי המגזר הפרטי:[37] הקמת צוות תגובה ביטחוני לתקיפות סייבר על בסיס CERT אקדמי; תוכנית להפחתת הסיכון הביטחוני ונקודות הכשל הלאומיות אל מול איומי סייבר; תוכנית לאומית להכשרה וליצירת מודעות בהקשרי ביטחון סייבר; שיפור אבטחת מרחב הסייבר הממשלתי; שיתוף פעולה

---

32 ראו ההגדרה המלאה בחוק: "Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems": "Public Law 107-296: Homeland Security Act of 2002 – Critical Infrastructure Information Act", *U.S. Congress*, 2002, Sec. 211/3.

33 שם, פרק 211/6.

34 "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection", *U.S. Department of Homeland Security*, 2003, §12

35 שם, סעיף 13.

36 על העיסוק בסוגיית ההרתעה בסייבר ראו, למשל: Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace", *International Security*, 41, no. 3 (2016-2017), pp. 44-71.

37 "The National Strategy to Secure Cyberspace", *U.S. White House*, 2003, p. X.

בין־לאומי לצורך שיפור הביטחון הלאומי בסייבר; הקמת שני מוסדות לשיפור הפיקוח על רמת האבטחה של התשתיות הממוחשבות הפיננסיות.[38]

האסטרטגיה הלאומית לאבטחת מרחב הסייבר כללה מרכיב נוסף, שנבע מההבנה שהעלייה הגבוהה במסחר בסייבר גורמת לרגישות מדינית נוספת כתוצאה מהיכולת לפגוע במדינות באמצעות פגיעה באינטרסים הכלכליים שלהן – דבר שהופך את המגזר הפרטי לשותף הכרחי ליצירת ביטחון ולשימור הריבונות. גישה זו קיבלה משנה תוקף בהחלטה הנשיאותית EO 13286 משנת 2003, שהובילה לשינוי ארגוני נוסף: מינוי גורמים רשמיים לגישור בין המגזר הביטחוני ובין המגזר הפרטי, על בסיס ארגונים אזרחיים, כגון "המועצה המייעצת לתשתיות לאומיות" (National Infrastructure Advisory Council" – NIAC), ו"המרכז לשיתוף וניתוח מידע" ("Information Sharing and Analysis Center" – ISAC).[39] למרות חשיבותו של המגזר הפרטי, קוצר היריעה של מאמר זה, המתמקד בשינוי בארגון הכוח הצבאי וזרועות הביטחון, לא מאפשר להרחיב על השינוי הארגוני שנוצר לצורך הרחבת שיתוף הפעולה בין המגזר הביטחוני ובין המגזר הפרטי בארצות הברית, שיתוף פעולה המהווה כיום גורם מרכזי בניטור האיומים במרחב הסייבר שם.

חוק נוסף, משנת 2004, נועד ליצור רפורמה בכלל שירותי המודיעין האמריקאיים ולהתאים אותם לאיומים העכשוויים.[40] החוק כלל לראשונה התייחסות גלויה לאפשרות שארצות הברית תעשה שימוש פסיבי ואקטיבי בתקשורת מתווכת מחשב כדי לשפר את ההגנה על עצמה. החוק גם מזכיר שני סוגי פעולות שונות במרחב הסייבר: פעולה התקפית נגד עסקאות ממוחשבות המתבצעות באמצעים אלקטרוניים, שנועדו למימון פשיעה וטרור חוצי גבולות; פעולת מודיעין לאיסוף מידע הקיים במרחב הסייבר לצורך מניעת כניסתם לארצות הברית של אנשים המשתייכים לארגוני טרור ופשיעה.[41]

בשנת 2006 פורסמה "התוכנית להגנה על תשתיות לאומיות" (National Infrastructure Protection Plan" – NIPP)[42] שיישמה את תהליכי הארגון שצוינו לעיל וקבעה את המשרד להגנת המולדת כגוף המתאם וקובע המדיניות להגנה על תשתיות לאומיות ומשאבים חיוניים, ובכלל זה מתאם בין הגורמים המדיניים

38 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 56.

39 "Executive Order No. 13286: Critical Infrastructure Protection in the Information Age", *The White House*, 2003.

40 "Public-Law 108-458: Intelligence Reform and Terrorism Prevention Act of 2004", *U.S. Congress*, 2004.

41 שם, פרק 6302, סעיף b1.

42 המסמך מחייב הערכת מצב עיתית, שנוסח מעודכן שלה יפורסם כל כמה שנים. מאמר זה מסתמך על גרסה מאוחרת יותר של המסמך משנת 2009: "National Infrastructure Protection Plan", *U.S. Department of Homeland Security*, 2009.

האזרחיים לגורמים הצבאיים והמודיעיניים. בתוכנית הוגדר לראשונה מרחב הסייבר כתשתית לאומית חיונית שיש להגן עליה, ולא רק ככלי תיווך שבאמצעותו תתבצע הפגיעה בתשתיות.[43]

המעבר מהחלטות מדיניות לארגון מחדש של הכוח הצבאי התרחש בשנת 2006 בעקבות המסמך "אסטרטגיה צבאית לאומית למבצעי סייבר" (National Military Strategy for Cyberspace Operations"), שנועד להגדיר את הידע הצבאי הנדרש לצורך שילובו של הצבא האמריקאי במאמצים להגן על מרחב הסייבר. המסמך הגדיר את ההקשר האסטרטגי, את הרגישויות ואת קווי המִתאר לגיבוש תוכניות פעולה ודוקטרינה ייחודית לפעילות צבאית סדורה במרחב הסייבר,[44] אך לא קבע את הקמתו של גוף פיקודי כללי ייעודי לנושא זה.

2012–2008: התפיסה המרחבית

תקופה זו מהווה את שיאו של השינוי המוסדי בארגון הפעלת הכוח האמריקאי בממד הסייבר. שינוי זה מתאפיין בשני עקרונות הנובעים מהגישה הרואה בסייבר מרחב בעל חשיבות צבאית: ארגון הכוח הצבאי על בסיס תפיסה מרחבית (Cyberspace); ממד הסייבר כמקור מידע ואינטראקציה חברתית ופוליטית, הדורש ניטור ופיקוח לצורך שימור הביטחון המדיני והאינטרסים הלאומיים.

את ניצני ההתייחסות של הממשל האמריקאי לאינטרנט כאל מרחב בעל מאפיינים ומורכבות ספציפיים, הדורשים התאמה ביורוקרטית ייחודית, ניתן לאתר במסמכים שליוו את הבחירות לנשיאות בשנת 2008 (אובמה מול מקיין). תשומת הלב הציבורית הפכה את המדיניות הנוגעת למרחב הסייבר, ובמיוחד את הממד הביטחוני שלה, לאחת הסוגיות המרכזיות של אותה תקופה. בעקבותיה פרסם "המרכז ללימודים אסטרטגיים ובין־לאומיים" (Center for Strategic and International Studies" – CSIS) דוח של מומחים בתחום ביטחון הסייבר שיועד לנשיא ה־44 של ארצות הברית.[45] הדוח קרא להגברת המעורבות של הממשל הפדרלי במרחב הסייבר ויצא נגד הגישה המסתמכת על הסדרה פנימית שלו בהובלת המגזר הפרטי. בין המלצות הדוח הייתה גם קריאה ליצירת מאזן הרתעה מול יריבים בתחום הסייבר.

43 שם, סעיף 3.2.5.

44 "The National Military Strategy for Cyberspace Operations", *U.S. Office of the Joint Chiefs of Staff*, 2006, p. 1.

45 "CSIS Commission on Cybersecurity for the 44th Presidency: Securing Cyberspace", *Center for Strategic and International Studies*, 2008.

בשנת 2009, עם תחילת כהונתו, פרסם ממשל אובמה מדיניות חדשה בתחום הסייבר תחת הכותרת "Comprehensive National Cyber Initiative" (CNCI).[46] מטרותיה המוצהרות של התוכנית היו להניע מהלך בין־סוכנותי נרחב במטרה לשפר את תחושת הביטחון במרחב הסייבר בקרב אזרחי ארצות הברית.[47] במסגרת זו הצהירה התוכנית על שינוי ארגוני באופן ניהול ההתמודדות עם האיומים בסייבר, תוך חלוקה לשני מאמצים מרכזיים: שיפור הריכוזיות באופן שיעלה את רמת השליטה והבקרה המדינית בממד הסייבר; תכנון אסטרטגי וניהול שותפויות עם גורמים בין־לאומיים בתחום זה. שיפור הריכוזיות בא לידי ביטוי בפיתוח טכני של מערכות שליטה ובקרה על רשתות המידע והמחשוב הפדרליות.[48] התכנון האסטרטגי בא לידי ביטוי בהקמת מוסדות לפיתוח ורכש לטווח ארוך שימנעו, בין השאר, חדירה של רכיבי חומרת מחשב נגועים, ובקביעת יעדים לחינוך של עובדי הממשל למודעות להגנה מפני איומי סייבר.[49] שותפויות בין־לאומיות כוננו עם גורמים שונים בזירה הגלובלית (מדינות, חברות וארגונים) במטרה ליצור יכולת הרתעה בתחום הסייבר.[50]

הצורך בתכנון אסטרטגי קבוע וסדור, מרמת מוסד הנשיאות ומטה, מצא ביטוי בשורת מסמכים שנכתבו בתחילת כהונתו של ממשל אובמה, ובכלל זה במסמך יסוד שפורסם תחת הכותרת "Cyberspace Policy Review". המסמך המליץ על כינון משרד לביטחון בסייבר (The Cybersecurity Office) כחלק מצוות היועצים של הנשיא ובשילוב עם "המועצה לביטחון לאומי".[51] ההמלצה יושמה בחוק משנת 2009 "United States Information and Communications Enhancement – Act"[52] – שגם קבע כי בראש המשרד לביטחון בסייבר יעמוד יועץ הנשיא לביטחון

---

46 התוכנית הייתה למעשה יישום של החלטה NSPD54 של הנשיא בוש, אותה אימץ הנשיא אובמה. נכללו בה חלק מההמלצות של דוח CSIS. ראו: "Comprehensive National Cybersecurity Initiative", *U.S. White House*, 2009, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

47 מכיוון שהתוכנית הייתה יישום של החלטה NSPD54, שהייתה חשאית בעיקרה והתמקדה על פי הפרסומים גם במהלכים ביטחוניים התקפיים ומודיעיניים, ניתן להניח שהיו לה גם מטרות לא גלויות.

48 "Comprehensive National Cybersecurity Initiative", pp. 2-3.

49 שם, עמ' 4–7.

50 שם, עמ' 5.

51 "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", *U.S. White House*, 2009, p. 7.

52 הרקע לחוק היה שימוע שנערך בסנאט בשנת 2008 על יכולות ההגנה על תשתיות ה־IT הפדרליות והביקורת שנמתחה על חוק FISMA מ־2002, שבבסיסה עמדה הטענה שהמדדים שהוא מציב לבדיקה עמומים וכי לא ברור לכול סוכנות מה היקף המידע עליו היא אמורה לפקח: "Information and Communications Enhancement Act of 2009 (S.921/ ICE Act)", *U.S Congress*, Sec. 2/4, 5.

קיברנטי, שישמש כחלק מצוות היועצים המצומצם שלו.[53] חשיבות הקמתו של המשרד לביטחון בסייבר הייתה בשיפור התיאום ויכולת המימוש של מדיניות ביטחונית כוללת מרמת הנשיא (המפקד העליון של כוחות הצבא האמריקאי), דרך סוכנויות הביטחון השונות ועד ליחידות הצבא, ובמיוחד ביכולת לגבש מדדים לפיקוח שיתבססו על פיתוח סטנדרטים לאבטחה במרחב הסייבר בכלל, ובמערכות מידע לאומיות בפרט.[54]

תוצאה משמעותית נוספת של המהלך ליצירת ריכוזיות בתחום הסייבר הייתה שיפור היכולת לגבש מדיניות להפעלת כוח לגיטימית בסייבר. זאת, כפועל יוצא של מדיניות תגובה סדורה שבראשה עומד הנשיא, על בסיס דוח של "המועצה המדעית הלאומית של ארצות הברית" ("U.S. National Science Council"),[55] שניתח את המשמעויות המשפטיות והאתיות של התקפות סייבר והמליץ כי התקפות כאלו ייחשבו כ"שימוש בכוח", דהיינו פעולה המצדיקה מענה מלחמתי (בממד הפיזי).[56]

הביטוי המשמעותי ביותר לשינוי הארגוני־תפיסתי שחל בארצות הברית ביחס לצורך להתמודד עם האינטרנט כמרחב הוא בשינוי בארגון הכוח הצבאי ובדוקטרינה להפעלתו. השינוי הארגוני הבולט בכוח הצבאי האמריקאי, המבטא את התאמתו להכרה בקיומו של מרחב סייבר, הוא ההקמה הרשמית של "פיקוד הסייבר של ארצות הברית" (CYBERCOM). ההחלטה על הקמת הפיקוד התקבלה בשנת 2009, והוא הוכרז כמבצעי שנה אחר כך והוכפף תחת "הפיקוד האסטרטגי של צבא ארצות הברית" (STRATCOM).[57] הפיקוד החדש הוגדר כ"תת־פיקוד אחוד" (Sub-Unified/Subordinated Command), כלומר גוף צבאי המוקם בהוראת הנשיא, כפיקוד המופקד על משימה מרחבית מוגדרת הדורשת התמחות מקומית, ופועל תחת פיקוד מרחבי של הצבא האמריקאי.[58]

יחידות ללוחמה באמצעות מחשבים ורשתות תקשורת ממוחשבות כבר היו קיימות בארצות הברית מאז שנות התשעים של המאה הקודמת (ראו ההתייחסות לעיל ליחידה 609), אך הקמת תת־פיקוד מרחבי לצורך זה ביטאה שינוי תפיסתי בעל משמעויות סמליות וארגוניות עמוקות. מבחינה ארגונית, למרות שעדיין

---

53 שם, פרק 3552.

54 שם, פרק 3556.

55 הדוח המקיף נכתב על ידי ועדה ייעודית לנושא, שהוקמה על ידי "המועצה המדעית הלאומית של ארצות הברית", והוא מנתח היבטים רבים נוספים הקשורים לתקיפות מקוונות, בתחום המשפט הפלילי והאזרחי.

56 "Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities", *U.S. National Science Council*, 2009, pp. 33-34.

57 "U.S. Cyber Command Fact Sheet", *U.S. Department of Defense*, 2010.

58 תתי־פיקוד מרחביים נוספים בצבא האמריקאי הוקמו לניהול הביטחון באלסקה, לסיוע לקוריאה הדרומית וללחימה באפגניסטן: "Joint Publication 1", *U.S. Office of the Joint Chiefs of Staff*, 2009, p. V-9.

לא הוקם פיקוד מרחבי מלא או זרוע/חיל למבצעים בתחום הסייבר,[59] הפיקוד הצבאי החדש הוא היום הגורם המנחה והמסנכרן את כלל המבצעים הצבאיים של ארצות הברית במרחב הסייבר, וכפופות אליו מבחינה מקצועית מפקדות ללוחמה מקוונת בזרועות ובחילות השונים (ים, אוויר, יבשה, נחתים). בנוסף לכך, "פיקוד הסייבר של ארצות הברית" אחראי לאיתור ופיתוח כוח האדם ואמצעי הלחימה ולגיבוש הדוקטרינה בתחום הסייבר. להקמת הפיקוד ניתן הד תקשורתי ובין־לאומי נרחב, והוא הפך לסמל מבחינת האופן הברור והגלוי שבו המחישה ארצות הברית למדינות אחרות את השלב המתקדם בו היא נמצאת במיליטריזציה של מרחב הסייבר. מעמדה זה של ארצות הברית כמעצמה צבאית מובילה (ואולי אף יחידה) בתחום הלחימה בסייבר הביא לשינויים ארגוניים דומים בקרב צבאות של מדינות נוספות ברחבי העולם (כמו, למשל, הקמת פיקוד הסייבר הסיני בשנת 2010).[60]

את השינוי הארגוני, ששיאו היה הקמת "פיקוד הסייבר של ארצות הברית", ליווה וייתכן שאף הוביל שינוי בדוקטרינה הצבאית, שפורסם במסמכים רשמיים של המטות המשולבים של ארצות הברית. אמנם, ההכרה במרחב הסייבר כמרחב שבו מתבצעת לחימה במקביל ובנוסף למרחבי הלחימה הקיימים החלה עוד בשנת 2006, אך נראה כי הידע שנצבר לא הבשיל לכדי דוקטרינה סדורה עד לפרסום עיקרי הדוקטרינה החדשה בשנת 2012,[61] שמטרתה הייתה מתן הנחייה אחודה לצבא האמריקאי כיצד לבצע מבצעי לחימה הגנתיים והתקפיים במרחב הסייבר.[62]

רמת הבשלות הגבוהה בפיתוח אמצעים, בהכשרת כוח אדם ובניסוח תורת לחימה ייחודית למרחב הסייבר, אליה הגיע הממסד הביטחוני האמריקאי מאז הקמת הפיקוד, נחשפה בהוראה הנשיאותית מספר 20 של הנשיא אובמה משנת 2012, העוסקת בפעילות התקפית בתחום הסייבר, לרבות "הגנה אקטיבית".[63] המסמך, המסווג "סודי", פורסם בעיתון הבריטי *The Guardian* כחלק ממצגות ומסמכים

---

59 הפיקודים בצבא האמריקאי נחלקים לפיקודים מרחביים האחראים להפעלת הכוח באזורים שונים בעולם (למשל, פיקוד המרכז, CENTCOM, המופקד על המזרח התיכון), ולפיקודים פונקציונליים־ייעודיים האחראים על בניין כוח, הכשרה והקצאת כוחות (למשל, פיקוד הכוחות המיוחדים, SOCOM). תחת סוג שני זה של פיקודים גם ניתן למנות את החילות ה"קלאסיים", כגון אוויר, ים ויבשה.

60 Tania Branigan, "Chinese Army to Target Cyber War Threat", *The Guardian*, July 22, 2010.

61 "Joint Publication 3-13 Information Operation", *U.S. Office of the Joint Chiefs of Staff*, 2012.

62 "Compendium of Key Joint Doctrine Publications", *U.S. Office of the Joint Chiefs of Staff*, 2014.

63 "Presidential Policy Directive 20: U.S. Cyber Operations Policy", *U.S. White House*, 2012.

סודיים שחשף והדליף אדוארד סנאודן,[64] והוא מהווה עדות משמעותית לשינוי המוסדי שעברה מערכת הביטחון האמריקאית ביחסה לתקשורת מתָווכת מחשב, עד לראייתה כמרחב פעילות. ההוראה הנשיאותית כוללת הגדרות מפורטות של סוגי תקיפות ומהלכי הגנה בסייבר, ובהם: הגנת רשתות פסיבית; פעילות סייבר התקפית; מבצעי השפעה בסייבר; איסוף מודיעין מתוך או באמצעות מרחב הסייבר; לוחמת סייבר לצורך הגנה; פעולות הגנה לא פולשניות; פעולות סייבר לחירום ועוד.[65] ההוראה מתייחסת לכך שכבר קיימות יכולות התקפיות מוכחות של ארצות הברית, אותן היא מפעילה כחלק מיישום זכותה להגנה עצמית, וזאת לאחר תהליך קפדני של אישורים.[66]

שינוי תפיסתי וארגוני נוסף שהחל בתקופה זו, מעֵבר לתפיסת הסייבר כמרחב מקביל למרחבים פיזיים, היה תחילתה של התייחסות אל מרחב הסייבר גם כאל זירה חברתית־ציבורית מרכזית, המגלמת בתוכה פוטנציאל שלילי וחיובי ודורשת ניטור והגנה. להגדרת מרחב הסייבר כתשתית העומדת בפני עצמה, שאינה רק מרחב המתווך בין אינטרסים במרחב הפיזי, נוספה בשנת 2010 הגדרה חדשה, כחלק מתוכנית המדיניות של המשרד לביטחון המולדת, שנקראה "Securing the Nation's Critical Cyber Infrastructure". תוכנית זו התייחסה אל מרחב הסייבר כזירה חברתית פוליטית וכלכלית העומדת בפני עצמה, שבתוכה נכללים מדינות, גורמי פשיעה, ארגוני טרור ויחידים.[67]

העיסוק הביטחוני באינטראקציה החברתית במרחב הסייבר השפיע גם על עדכון הדוקטרינה של צבא ארצות הברית שעסקה בהוצאה לפועל של מבצעי תודעה (Information Operations). במסמך דוקטרינרי גלוי משנת 2012 נאמר כי הסייבר הוא מרחב חיוני לקיומם של מבצעי תודעה, כחלק ממאמץ צבאי מתמשך,[68] וכי הוא נתפס כאחד הערוצים להשפעה על "סביבת המידע". זאת, הן ביכולת לעשות בו או דרכו שימוש כדי לשבש ולמנוע מסרים, והן ביכולת להחדיר מסרים או לבצע הונאה, תוך שימוש במדיה חברתית.[69] הפיכתו של מרחב הסייבר לחלק

64 אדוארד סנאודן הוא עובד לשעבר של סוכנויות המודיעין האמריקאיות CIA ו־NSA, שהתמחה במודיעין מקוון. סנאודן הדליף בשנת 2012 כמות גדולה של מסמכים לגורמי תקשורת מובילים בעולם. המסמכים חשפו את עומק האיסוף המודיעיני והפעולות האקטיביות שנוקטות ארצות הברית ובעלות בריתה (קהילת המודיעין המשותפת לבריטניה, קנדה, ניו זילנד ואוסטרליה) במרחב הסייבר.

65 "Presidential Policy Directive 20: U.S. Cyber Operations Policy", pp. 2-4.

66 שם, עמ' 4–11.

67 "Securing the Nation's Critical Cyber Infrastructure" *U.S. Department of Homeland Security*, 2010, pp. 7-10.

68 "Joint Publication 3-13: Information Operations", *U.S. Office of the Joint Chiefs of Staff*, 2012, p. III.

69 שם, עמ' II–9.

מתחומי הפעולה של הצבא האמריקאי מתברר גם מאופן ההתייחסות אליו במצגות רשמיות של הפיקודים המרחביים של צבא ארצות הברית, שם הוא מוצג כחלק בסיסי מתפיסת הפעולה האופרטיבית.[70]

לצד זאת, ארצות הברית מכירה בכך שמבחינה ארגונית, היכולת לפעול במרחב הסייבר הציבורי־אזרחי אינה בלעדית לה, ולכן עליה לשתף פעולה עם גורמים תת־מדינתיים ועל־מדינתיים, ובעיקר עם חברות ייעוץ ותוכנה מקומיות ובין־לאומיות, המהוות שותף ומקור מידע לצורך שיפור האבטחה במרחב הסייבר, כפי שעולה גם מהמלצות של ועדות ודוחות רשמיים שונים בארצות הברית.[71] כך, למשל, מהמלצות אלו עולה כי למרות התמורות הארגוניות שהובילו להכשרת כוח אדם צבאי וממשלתי ייעודי לתחום הסייבר, עדיין נותרו תחומים שבהם ישנו יתרון לגורמים חיצוניים שאינם צבאיים, וכי אין לארצות הברית יכולת לגשר על פער זה בתקופה הקרובה, ולפיכך עליה להסתמך על היתרון היחסי של גורמים חיצוניים אלה. מדובר במיוחד בתחומים כגון זיהוי פוֹרֶנזי, שניכר כי עדיין לא נמצא להם פתרון בדרג המדינתי.[72]

בניין הכוח בסייבר כביטוי לשינוי תפיסתי ארגוני

בפברואר 2016 פרסם הנשיא אובמה מאמר דעה בעיתון *Wall Street Journal*, בו טען כי יש להגדיל את ההשקעה התקציבית של ארצות הברית בפיתוח טכנולוגיות להגנה בסייבר, בדגש על תשתיות של מערכות מידע ממשלתיות.[73] פרסום המאמר הקדים במעט את החלטת הממשל האמריקאי להגדיל את ההוצאות על פיתוח טכנולוגיות אלו ב־19 מיליארד דולר.[74] התפיסה המוצגת במאמר של אובמה מייצגת גישה הפוכה לתהליך שתואר במאמר זה, והיא רווחת עדיין בקרב רבים ממקבלי ההחלטות בארצות הברית, וככול הנראה גם במדינות נוספות. במוקדה נמצאת ההנחה כי הגברַת הפיתוח הטכנולוגי והשקעת משאבים נוספים בו הן

70 למשל, במצגת קונצפטואלית לא מסווגת שהוכנה עבור גנרל מולטון, ראש מרכז התכנון והמבצעים של הפיקוד האירופי של צבא ארצות הברית, להצגה במכללה לקצינים של צבא היבשה: "The Operational Art of Fighting In and Through Cyberspace (Unclassified PP presentation)", *U.S. European Command*, Slide 12.

71 "CSIS Commission on Cybersecurity for the 44th Presidency: Human Capital Crisis in Cybersecurity", *Center for Strategic and International Studies*, 2010, p. VIII.

72 למשל, פעילות וירוס נחשפה על ידי חברות מסחריות המתמחות בכך, כגון מעבדות קספרסקי ואחרות.

73 Barak Obama, "Protecting U.S. Innovation from Cyberthreat", *Wall Street Journal*, February 9, 2016, http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003.

74 Tobias Naegele, "7 Keys to President Obama's 19 Billion Cybersecurity Plan", *GOVTECH Works*, February 16, 2016, https://www.govtechworks.com/7-keys-to-obama-19-billion-cybersecurity-plan/#gs.iMSThHM.

המזוֹר לקשיים הגוברים של ארצות הברית לספק ביטחון במרחב הסייבר ולהגן על תשתיות לאומיות ומשאבים חיוניים. למרות שמאמר הדעה של אובמה מתייחס לכך שהגישה הארגונית המרחבית יושמה על ידי בכירי מערכת הביטחון והצבא האמריקאיים, נראה כי גם היום אין זו התפיסה הרווחת בקרב כלל מקבלי ההחלטות בארצות הברית.

הדיון שלהלן יעסוק בחלופה להשקעה עיקרית בפיתוח הטכנולוגי, לעומת החלופה להשקעה גם בפיתוח ארגוני, ויעמוד על המשמעויות האפשריות של שתי החלופות. אף שאין מדובר בסקירה השוואתית, יש בדיון זה ערך להבנת עמדתן של מדינות אחרות החותרות להשגת יתרון ביטחוני במרחב הסייבר ונוקטות גם הן מדיניות של העדפת הפיתוח הטכנולוגי על פני פיתוח הארגון והתפיסה.

כפי שצוין, מחקרים בתחום לימודי הביטחון והיחסים הבין־לאומיים שנעשו בשנים האחרונות עסקו רבות בהתפתחות צורת הלחימה בסייבר, באסטרטגיה המדינתית הרצויה במרחב זה ובאמצעי הלחימה למימושה.[75] לכן, יש לחזור ולשאול מהי החשיבות של התמקדות בשינוי הארגוני והתפיסתי בעת הזאת לעומת ההתמקדות בפיתוח טכנולוגי, ובאופן ספציפי: מהי דרך ההתארגנות המיטבית להשגת יתרון ביטחוני במרחב הסייבר ומהי התרומה שבתיאור תהליך זה להבנה ולשיפור היכולת של מדינות להעניק ביטחון לאזרחיהן אל מול האיומים הגלומים בממד הסייבר?

בפתח המאמר צוין כי בעת הזו יש להתמקד בארגון הכוחות הפועלים להחיל ביטחון במרחב הסייבר ולבנות את תפיסת ההפעלה שלהם על בסיס הגישה הצבאית האמריקאית, הרואה בסייבר מרחב לחימה מקביל למרחבים הפיזיים. הצורך בהתמקדות זו נעוץ בשני גורמים משלימים: התעצמות האיומים הנובעים ממרחב הסייבר והשינויים שחלו בהם; המאפיינים הטכנולוגיים הייחודיים של אמצעי הלחימה במרחב הסייבר.

באשר לגורם הראשון – השינוי בתפיסת האיום – הדוגמאות מתוך שלוש התקופות שתוארו לעיל ממחישות את השינוי הארגוני שחל בממסד הביטחוני האמריקאי כביטוי להפנמה גוברת של עומקו ומהותו של האיום הגלום במרחב הסייבר על מדיניות הביטחון בכלל ועל יכולת הפעלת הכוח הצבאי בפרט. מקור השינוי הוא במעבר מתפיסת מרחב הסייבר כמערכת להעברת מידע אל תפיסתו כמרכיב מהותי בחיים המודרניים: מאיום על מידע מדינתי רגיש וחשאי מטבעו (מידע

---

75 ראו, למשל, הדיון על יכולת ההתגוננות מול מתקפות סייבר, תוך ניצול תקשורת מחשב המשמשת מכשירים ("האינטרנט של הדברים"): Bruce Schneier, "Security and the Internet of Things", *Schneier on Security*, 2016, https://www.schneier.com/blog/archives/2017/02/security_and_th.html; וכן הדיון על יכולת ההרתעה בסייבר: Nye, "Deterrence and Dissuasion in Cyberspace", pp. 44-71.

מדיני רשמי, מודיעין, ידע טכנולוגי וכדומה) מצד מדינות אחרות או פרטים, שניתן להגדירו כחלק מ"אבטחת מידע", לאיום על התשתיות הבסיסיות ומשאבי היסוד של המדינה המודרנית הנשענים על תשתיות מידע ממוחשב, שניתן להגדירו כחלק מהגנה על תשתיות ואתרים אסטרטגיים ("הגנה אזרחית"), וממנו לאיום מרחבי ("מרחב הסייבר") המשיק ומשפיע על חלק גדול מהפעולות האזרחיות והצבאיות של מדינות במרחבים הפיזיים, שניתן להגדירו כאיום על ריבונות המדינה וקיומה ועל האינטראקציה הבין־אישית – כלכלית, פוליטית וחברתית – קרי, על ביטחון החברה והציבור. השימוש האנושי המגוון במרחב הסייבר, המהווה חלק משמעותי בהתקשרות חברתית, כלכלית ופוליטית, אינו מאפשר עוד להתמקד בהגנה על תשתיות מדינתיות באמצעות פיתוח טכנולוגי בלבד (כפי שמשתמע מהצהרתו של הנשיא אובמה). לעומת זאת, תפיסה הרואה במרחב הסייבר מרחב פיזי מאפשרת הגדרת יעדים ומטרות לפעולה שמכילים את מגוון האינטראקציות הללו.

הגורם השני הוא, כאמור, הייחודיות הטכנולוגית של אמצעי הלחימה במרחב הסייבר, הנובעת ממהירות ההתפתחויות הטכנולוגיות בתחום זה ומזמינותם של אמצעי הלחימה בשוק הפרטי. הצורך לעדכן חומרה ותוכנה בקצב מהיר במערכת המחשב הביתית גורם תסכול לרבים, לא כל שכן כשמדובר בביטחון המדינתי בתחום הסייבר: התפתחות אמצעי הלחימה והריגול הממוחשבים, הניתנים לרכישה בקלות יחסית במגזר הפרטי, יחד עם פשטות הפעלתם,[76] פוגעות ביכולת של מדינות להשיג יתרון טכנולוגי באמצעות פיתוח אמצעי לחימה חדשים. מערכות הפיתוח המדינתיות מתקשות להתמודד עם קצב הפיתוח והזמינות של אמצעים דומים בשוק הפרטי, ולכן פיתוח בלבד אינו יכול להיות הדרך היחידה או אף העיקרית להשגת יתרון בתחום זה. מאפיין ייחודי זה הוא שמוביל למסקנה שיכולת השליטה וההגנה על ביטחון מרחב הסייבר לא יכולה להתבסס רק על שכלול טכנולוגי של אמצעי לחימה, אלא חייבת לכלול גם את ארגון הכוח ופיתוח תפיסה ודוקטרינה להפעלתו, באופן שישלב אותן עם הפעולות הצבאיות הנוספות של המדינה להגברת הביטחון ולשימור הריבונות. גישה זו דומה להתארגנות ליצירת ביטחון במרחבים פיזיים, כגון ארגון הכוח האווירי להגנה על המרחב האווירי. ההקבלה המוצגת במאמר זה בין המרחב הווירטואלי ובין המרחב הפיזי – בין תחום הנתפס כחדש ומהפכני לבין צורת הפעולה "הישנה והשמרנית" – היא חלק מהפתרון הנדרש.

מהסקירה לעיל עולה כי הגישה הארגונית המרחבית היא למעשה הגישה אותה מיישמת הביורוקרטיה הביטחונית (במיוחד הצבאית) האמריקאית. הביטוי המעשי לה הוא כינון ממסד ביטחוני ייעודי רחב ואיתן במרחב הסייבר, הכולל כוח אדם ייעודי רב הפועל באופן הירכי – מרמת משרד היועץ במטה הנשיא, דרך יחידות

76 סוגיה זו כבר זכתה להכרה על ידי הממשל האמריקאי. ראו, למשל: "Securing the Nation's Critical Cyber Infrastructure", p. 3, Figure 1.

צבאיות וכלה במערך פיקוד צבאי ושליטה לאומי (US-CERT), תוך תיאום עם יחידות שיטור וחטיבות במשרד להגנת המולדת ועם גופים סמי־ממשליים המגשרים בין האוכלוסייה האזרחית (NIAC, NCSC), כולל המגזר העסקי והאקדמיה (ISAC), ובין הממשל. צעדים אלה מעידים על הפנמת חשיבותו של מרחב הסייבר לצורך הגנה והשפעה על ציבורים שונים. הפנמה זו הובילה, כאמור, גם לשינוי במאפייני הפעלת הכוח בסייבר – מפעולות להשגת מידע רגיש שיאפשר יכולת פיתוח, פעולה או הרתעה באמצעות "כוח קשה" קינטי או אחר, לאיום ב"כוח רך", המשפיע על תודעת היריב, על הלגיטימציה לחופש הפעולה הצבאי והביטחוני שלו, ואף על הפעולות המתקיימות בתוך מרחב הסייבר, כגון העברת מידע ממוחשב, תקשורת ופעולות כלכליות ממוחשבות.

ייתכן כי השינוי הארגוני המרחבי הוא גם אחת הסיבות להירכיה ביחסי הכוחות בין מדינות שונות הפועלות במרחב הסייבר. זאת, משום ששינוי זה הוא אחד המאפיינים הייחודיים של מעצמות כמו ארצות הברית, המהוות כוח בין־לאומי ביטחוני מוביל גם במרחב הסייבר ומסוגלות להקצות את המשאבים לארגון הפעולה הצבאית על בסיס עיקרון מרחבי. שינוי זה הוא פעולה יקרה, הדורשת משאבי כוח אדם, חשיבה וארגון שהם ייחודיים למדינות מפותחות המורגלות בהוצאה ביטחונית גבוהה. במילים אחרות, פעולות אסימטריות במרחב הסייבר, כגון טרור, חבלה, גניבת מידע, לוחמה פסיכולוגית ותקשורת מוטת "Fake News", יכולות להתבצע על ידי מדינות חלשות וארגונים שאינם מדינות. לעומת זאת, היכולת לארגן את הפעולות במרחב הסייבר כפעולות צבאיות סדורות, על בסיס הגישה הארגונית המרחבית המאפיינת את הפעולות הצבאיות במרחבים הפיזיים, היא נחלתן של מעצמות עולמיות ואזוריות ועוד מספר מדינות בעלות צבאות מודרניים עתירי טכנולוגיה. השאלה האם אנו עדים לתחרות ארגונית בין הסגנון המערבי של ארגון הכוח בסייבר באמצעות כינון מוסדות צבאיים וביטחוניים מדינתיים רשמיים, שארצות הברית היא המובילה אותו, ובין תפיסות ארגון "היברידיות", קרי מימוש פעולות סייבר התקפיות באמצעות שילוב וסנכרון מוסדות ביטחון מדינתיים וגורמים אקדמיים, המגזר הפרטי וגורמי פשיעה, אותן מובילות מדינות כגון סין ורוסיה, דורשת מחקר נוסף שחשיבותו עולה כיום, כפי שמתברר ממאמר זה.

לאור יישום השינוי בארגון הסייבר ככוח צבאי, ראוי לשאול האם ניתן לבחון אותו באותם הכלים בהם אנו מודדים את בניין הכוח הצבאי במרחב הפיזי ולהשוותו אליו? התשובה לכך אינה חד־משמעית. מצד אחד, מבחינת חישובים של עלות לעומת תועלת, ברור שלא ניתן להשוות בין העלות של פלטפורמה אווירית חדשה, הן מבחינה כספית והן מבחינת משאבי הפיתוח וההשקעה המקצועית, ובין פיתוח כלי הפעולה בסייבר; מצד שני, בשני המקרים בניין הכוח טומן בחובו צורך לפתח את היכולת להפעיל את אמצעי הלחימה בשילוב ובהלימה לאמצעי

לחימה קיימים המיועדים ללחימה במרחב אחר, וזאת באמצעות נהלים, דוקטרינה וכלים טכנולוגיים המאפשרים פיקוד ושליטה משופרים. ניתן אף לערוך השוואה היסטורית בין הדברים – בין התפתחות מערכי לחימה צבאיים במרחבי האוויר והים ובין התפתחות מערכי הלחימה במרחב הסייבר בעקבות התפתחויות טכנולוגיות. השוואה כזאת מדגישה, כאמור, את חשיבות ארגון הכוח והתפיסה המרחבית בתחום הסייבר כדרך לבסס יתרון ביטחוני בין המדינות הפועלות במרחב זה.[77]

סיכום ומסקנות

השינוי הארגוני במרחב הסייבר בארצות הברית הוביל לתוצאות בשלושה תחומים: שינוי במנעד הפעולות בסייבר; שינוי במאפייניהן של פעולות אלו; שינוי בתפיסת הפעילות במרחב הסייבר והשלכותיה על תפיסת הביטחון הלאומית של ארצות הברית והאסטרטגיה רבתי שלה.

התפתחות מנעד הפעולות הביטחוניות של ארצות הברית במרחב הסייבר, ממצב מצומצם ומוגבל שהפעילות בו נועדה בעיקר לאבטח את מרחב הסייבר הלאומי (מוסדות ואינטרסים ברורים) ולהגן עליו, למצב שבו הסייבר ערוך לפעולה התקפית, הגנתית ומודיעינית כאחת, נובעת מהשינוי הארגוני. זה הוביל להקמת יחידות, סוכנויות וארגונים בעלי אחריות מוגדרת ומכניזם לאומי לתיאום הפעילות במרחב הסייבר. למרות התפתחות זו, השינוי הארגוני אינו זוכה להכרה מספקת (לא במחקר ולא במסגרות המקצועיות), והחלטות תקציביות משמעותיות, כגון זו של ממשל אובמה, מבטאות גישה לפיה הבסיס ליצירת ביטחון ויתרון במרחב הסייבר הוא קידום השקעות בפיתוח טכנולוגי גרידא. גישה זו סותרת את ההתפתחות המשמעותית בארגון מרחב הסייבר כפי שתוארה במאמר זה ומסכנת את המשכה. היא נובעת גם מגישה ביורוקרטית הנוטה להעריך מדיניות באמצעות מדדים כמותניים (עלות לעומת תועלת), תוך התעלמות מהיבטים איכותניים, כגון יצירת תפיסה, ארגון ודוקטרינה, שהם חלק ממרכיבי האיכות המעניקים יתרון למדינות בהפעלת אמצעי לחימה בכול מרחב, ובכלל זה במרחב הסייבר.

המסקנה הסופית של המאמר היא כי במסגרת תכנון האסטרטגיה הביטחונית היום, כדאי להתייחס גם למאפיינים ולהבדלים ביכולת לארגן את הפעולה הביטחונית במרחב הסייבר בין מדינות, בדגש על מעצמות אזוריות והכוחות הביטחוניים המובילים בעולם. תהליך הארגון וביסוס תפיסת הפעולה המרחבית, המאפיין את המדיניות הצבאית האמריקאית היום, הוא חלק מיצירה וביסוס של נורמות

77 שאלה זו החלה לקבל תשומת לב של חוקרים בשנים האחרונות. ראו, למשל: עמית שיניאק, "התהוות המדינה במרחב הספר המקוון: השוואה תיאורטית והיסטורית", **בין הקטבים**, מרכז דדו לחשיבה צבאית בין־תחומית, דצמבר 2014, עמ' 13–44; Florian Egloff, "Cybersecurity and the Age of Privateering: A Historical Analogy", *Cyber Studies Programme*, Working Paper Series No. 1, University of Oxford, March 2015.

התנהלות, ואף הסכמים בין מדינות, סביב כללי המשחק במרחב הסייבר. אלה נמצאים במוקד השיח הבין־לאומי סביב מרחב הסייבר כיום, וראוי שיילמדו, ייחקרו ויהוו חלק מהערכת העלות והתועלת בפיתוח יכולות בתחום זה. הגישה הנדרשת כיום, עליה ממליץ המאמר, היא גישה ארגונית המתבססת על השוואה מסוימת בין התנהלות של מדינות במרחב הסייבר ובין התנהלותן במרחבים פיזיים. גישה זאת מאפשרת פיתוח יכולות שליטה רב־ממדיות לניהול "קרב משולב" מסונכרן ומתואם בין מרחבי הלחימה השונים – הפיזיים והטכנולוגיים – ויצירת יתרון ביטחוני במרחב הסייבר.