תשתיות קריטיות והשפעת התלות ביניהן בעת תקיפה קיברנטית – המקרה האמריקאי

הראל מנשרי וגיל ברעם

השימוש הגובר בטכנולוגיית המידע בצד התלות הגדלה של השוק החופשי במוצרים ובשירותים שמסופקים בידי תשתיות, מגבירים את שכיחות התלות ההדדית בין התשתיות ומגבירים את חשיבותה של התופעה – פגיעה בתשתית קריטית עלולה להשפיע באופן מכריע על יכולותיהן של תשתיות נוספות לפעול ובמקרים רבים, עלולה פגיעה שכזו לגרום לקריסתן של תשתיות הקשורות לתשתית הנפגעת. התלות הקיימת בין התשתיות מחייבת את הגורמים העוסקים בתכנון תקיפה קיברנטית כמו גם את הגורמים העוסקים בהגנה להתאים עצמם למציאות זו ולהיערך בהתאם.

המאמר מתאר את המודלים הקיימים לניתוח מצבי תלות בין תשתיות, מציע מסגרת אנליטית לתיאור התלות ההדדית ביניהן ובוחן את האפשרויות העומדות בפני ארצות הברית בבואה לבצע תקיפה קיברנטית וההשלכות אותן עליה לקחת בחשבון.

מילות מפתח: תלות בין תשתיות; ארצות הברית; לוחמה קיברנטית; תשתיות חיוניות.

השימוש הגובר בטכנולוגיית המידע ובניטור ובקרה באמצעות מערכות בקרה ממוחשבות, בצד התלות ההולכת וגדלה של השוק החופשי במוצרים ובשירותים שמסופקים באמצעות תשתיות (למשל אנרגיה חשמלית), מגבירים את שכיחותה

ד"ר הראל מנשרי הוא עמית מחקר במכון לחקר מדיניות נגד טרור במרכז הבינתחומי בהרצליה. מאמר זה מבוסס על פרק מעבודת הדוקטורט שלו בנושא "שילוב לוחמה קיברנטית בסוגי לוחמה אחרים, חקר מקרה: ארצות הברית".

גיל ברעם היא דוקטורנטית בתוכנית המצטיינים בחוג למדע המדינה באוניברסיטת תל אביב וחוקרת בסדנת יובל נאמן למדע, טכנולוגיה וביטחון.

של התלות ההדדית בין התשתיות ואת חשיבותה של התופעה. פגיעה בתשתית קריטית עלולה להשפיע באופן מכריע גם על יכולותיהן של תשתיות נוספות לפעול, ובמקרים רבים היא עלולה לגרום לקריסתן של תשתיות הקשורות לתשתית הנפגעת.

מאז מתקפת הטרור ב־11 בספטמבר 2001 נקט הממשל האמריקאי סדרה של פעולות במטרה לשפר ולקדם נושאים ביטחוניים, בכלל זה הביטחון הקיברנטי. עוד בנובמבר 2002 חתם הנשיא ג'ורג' בוש על צו נשיאותי (*National Security Presidential Directive 16*) שהנחה את גופי הממשל, ובראשם המשרד לביטחון המולדת (Department of Homeland Security – DHS), לפתח לראשונה כללים ברמה הלאומית שיקבעו מתי ובאלו תנאים תוכל ארצות הברית לבצע תקיפות קיברנטיות משטחה.[1] בפברואר 2003 פרסם הבית הלבן מסמך בשם "האסטרטגיה הלאומית לביטחון המרחב הקיברנטי" (*The National Strategy to Secure Cyber Space*), שקבע כי הביטחון הקיברנטי הוא נושא הנתון תחת אחריותו של המשרד לביטחון המולדת. מטרת המסמך הייתה "ליצור את מסגרת הפעולה להגנה על התשתיות החיוניות לכלכלה, לביטחון ולדרך החיים האמריקאית". המסמך כלל טווח רחב של פעולות שנועדו להגן על ביטחונה הלאומי של ארצות הברית באמצעות הגנה על תשתיותיה הקריטיות המרכזיות. אסטרטגיה זו נועדה ליצור מסגרת עבודה שתגדיר לראשונה את סדר העדיפויות ותנחה את רשויות הממשל השונות כיצד לפעול כדי לחזק את הגנתן בתחום הקיברנטי.[2]

גם במהלך תקופת כהונתו של הנשיא אובמה התקיימה פעילות ענפה בתחום זה, בין היתר על ידי הדגשת חשיבותו של האיום הקיברנטי במסגרת "אסטרטגיית הביטחון הלאומי" (*National Security Strategy*), שפורסמה במאי 2010; בפרסום "האסטרטגיה הבין־לאומית למרחב הקיברנטי" (*International Strategy for Cyberspace*) במאי 2011, שהניחה את היסודות לדרכי פעולה ברורות בהתמודדות עם האיום הקיברנטי; בהצהרה שפורסמה מטעם הפנטגון על כך ש"גרימת נזק לארצות הברית במרחב הקיברנטי דינה כדין פעולה מלחמתית נגדה", ועוד.[3] בנובמבר 2014 הזהיר ראש הסוכנות לביטחון לאומי (NSA) מפני יכולותיהן של סין ושל "שתיים־שלוש מדינות נוספות" לפגוע, באמצעות תקיפות קיברנטיות, בתשתיות הקריטיות של ארצות הברית, בהן החשמל, התעופה והמערכות הפיננסיות.[4] הפעילות האחרונה של הממשל בנושא האיום הקיברנטי הייתה בינואר 2015, כאשר הנשיא אובמה פנה לקונגרס בקריאה לקידום חקיקה להתמודדות עם איום גובר זה.[5] הפעילות האמריקאית הרשמית ופרסומים נוספים מראים כי נושא הביטחון הקיברנטי ושאלת ההגנה על תשתיות לאומיות קריטיות נמצאים על סדר היום של מקבלי ההחלטות בארצות הברית כמעט שני עשורים וכי מדובר בתחום בעל חשיבות רבה לממשל האמריקאי.

התלות הקיימת בין התשתיות מחייבת את הגורמים העוסקים בתכנון תקיפה קיברנטית ומתכוונים לפעול נגד תשתיות זרות לבחון היטב את הקשרים בין התשתיות שבכוונתם לתקוף ובין תשתיות אחרות, הן במדינת היעד, הן בארצם שלהם והן במדינות אחרות. זאת, כדי למנוע פגיעה שתשפיע על התשתיות במדינת התוקפים, וכן למנוע פגיעה בתשתיות נוספות, העלולה להיחשב כפשע מלחמה. גם הגורמים העוסקים בהגנה על תשתיות קיברנטיות חייבים ללמוד ולמפות היטב את הקשרים והתלות בין התשתיות השונות, ליצור יתירויות ולמנוע קריסה "מתגלגלת" ("אפקט דומינו") של כלל התשתיות התלויות במקרה של פגיעה באחת מהן.

מטרתו של מאמר זה היא להציע מסגרת כללית לתיאור התלות ההדדית בין תשתיות ולבחון את האפשרויות העומדות בפני ארצות הברית בבואה לבצע תקיפה קיברנטית. תחילה מוצגים ומתוארים המודלים הקיימים לניתוח מצבי תלות בין תשתיות. יש לציין, בהקשר זה, כי אף על פי שמדובר במודלים שאינם חדשים, הם רלוונטיים מאוד לימינו. זאת, משום שכמעט ולא חלו שינויים בהתפתחותן ובמאפייני הפעולה של מרבית התשתיות במהלך העשור האחרון – דבר שמהווה נקודת תורפה משמעותית ומקל על ביצוע תקיפה קיברנטית נגדן. בהמשך המאמר נערך ניתוח של התלות ההדדית בין התשתיות במקרה האמריקאי ונבחנות ההשלכות אותן מקבלי ההחלטות בארצות הברית צריכים לקחת בחשבון. זאת, בנוסף לשיקולים כמו עצם פתיחת מערכה שתסכן את התשתיות האמריקאיות המקושרות לתשתיות אחרות וחשופות לתקיפה, בשל היותה של ארצות הברית מדינה כה מתקדמת מבחינה טכנולוגית.

פגיעה בתשתיות במצבי תלות

בין התשתיות של המדינות המתועשות דוגמת ארצות הברית לבין תשתיותיהן של מדינות אחרות קיימת זיקה, ולעתים מתקיימים גם יחסי תלות. הכלכלה הגלובלית ויחסי המסחר בין המדינות נשענים על פיתוחי התקשורת האלקטרונית, המאפשרים קיום קשרים, ביצוע תנועות מסחריות (טרנסקציות) והעברת מידע וידע מסביב לעולם כמעט במהירות האור. הקִדמה הטכנולוגית, בעיקר בתחומי התקשורת, מאפשרת לתאגידי ענק בין־לאומיים להפעיל ולתחזק את התשתיות במדינות רבות. גם תאגידים אמריקאיים משקיעים משאבים בתשתיות ובכלכלה של מדינות אחרות. קיומה של הכלכלה העולמית תלוי באספקה שוטפת של משאבי אנרגיה, כך למשל הכלכלה הסינית התלויה באספקה של משאבי אנרגיה מהמפרץ הפרסי. הקמתן של תשתיות קריטיות בכל תחומי התעשייה (כמו אנרגיה, מים, תחבורה וכדומה) מלווה בהשקעות כבדות וארוכות טווח. בנייתן של תשתיות אלו נמשכת שנים ארוכות, ולפיכך גם מערכות הניהול, הבקרה והשליטה שלהן (Supervisory Control And Data Acquisition – SCADA), המבוססות על בַּקרים

מתוכנתים תעשייתיים, אינן משתנות ואינן מתעדכנות לעתים מזומנות, בשונה מטְווחי הזמן התזזיתיים והמהירים המקובלים בעולם הקיברנטי הנוכחי. בהתאמה לכך, גם בחינת עמידותן של מערכות התשתית מבוססת על מודלים שמרניים, שעל אף הזמן שעבר מאז פותחו, הם עדיין תקפים ורלוונטיים.

על פי המודל של סטיבן רינאלדי[6] (שיתואר בהמשך), כאשר למדינות יש תשתיות משותפות – למשל, תשתיות חשמל, מים וגז – פגיעה בתשתית במדינה אחת עלולה להשפיע על התשתית במדינה האחרת. ברור שתשתיותיה וכלכלתה של ארצות הברית עלולות להיפגע פגיעה הרסנית אם ייפגעו תשתיות וכלכלות של מדינות אחרות המקושרות אליה.

במקביל לתלות הבין־מדינתית, קיימת תלות הדדית בין התשתיות בתוך המדינה עצמה. פגיעה באחת מהן עלולה לגרור תגובת שרשרת ו"אפקט דומינו" שבהם ייפגעו התשתיות בזו אחר זו. כך למשל:

א. תשתית המייצרת חשמל תלויה במשאב המסופק באמצעות תשתית אחרת המזרימה נפט או גז. פגיעה בתשתית הגז או הנפט תפגע בתשתית החשמל.

ב. פגיעה בתשתיות פיננסיות, דוגמת בורסה ובנקים, עשויה לגרור פגיעה בתשתיות נוספות, הנדרשות לתזרים מזומנים לצורך פעילותן. במקרה זה ייתכנו גם תרחישים של פגיעה בסדר הציבורי בשל בעיות כלכליות.

ג. פגיעה בתשתית הרכבות של ארצות הברית עלולה לפגוע קשות במסחר בארצות הברית ובכלכלתה, ותוך ימים ספורים אף לגרום למחסור במזון באזורים שונים במדינה.

ד. פגיעה בתחנת ייצור או השנאת חשמל בזמן עומס גדול עלולה לגרור תגובת שרשרת שבה "ייפלו" תחנות נוספות. אירוע כזה התרחש בארצות הברית באוגוסט 2003, כאשר כֶּשֶׁל תפעולי בתחנת השְׁנאה, שנבע מרשלנות, גרם ל"הפלת" מערכי ייצור ואספקת חשמל. זו הייתה הפסקת החשמל החמורה בתולדות צפון אמריקה – תושבים בצפון־מזרח ארצות הברית ובקנדה נותקו מרשת החשמל למשך שעות ארוכות, ובאזורים אחדים אף למשך ימים.[7]

ה. פגיעה בתשתית החשמל עלולה להשפיע באופן מידי על יתר התשתיות במרחב הארצי והעירוני: פגיעה בבתי חולים, הפסקת ייצור בתעשייה, פגיעה במערכות תקשורת ופגיעה במערכות תחבורה, בעיקר ביבשה, אך גם במערכות אוויריות מסוימות.

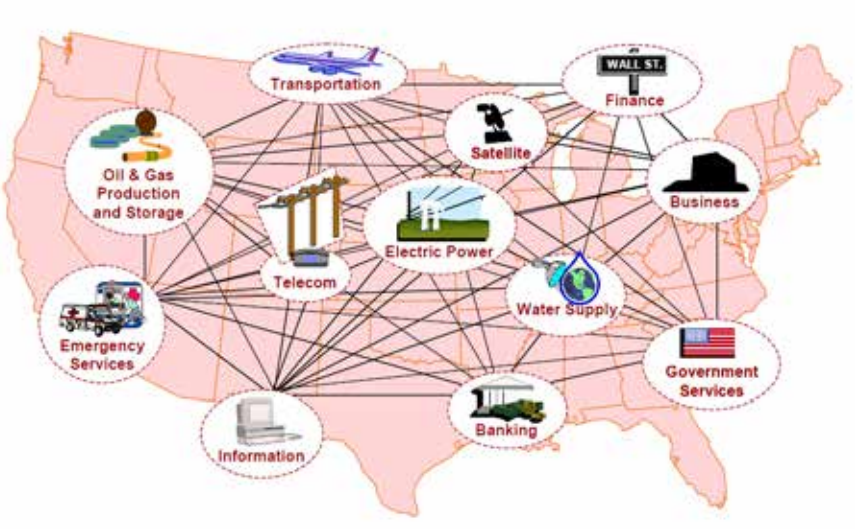
ו. פגיעה במערכת הרמזורים בנתיב תחבורה סואן תגרום לתגובת שרשרת תחבורתית, שתשפיע על מערכות נוספות שפעילותן תלויה בתשתיות תחבורה.

תוקף המתכנן תקיפה על תשתית חיונית של יריב צריך לבדוק במדוקדק כיצד תשתית זו קשורה לתשתיות אחרות וכיצד כל אלו תלויות האחת בשנייה. ניתן לעתים לבחון אפשרות לפגוע בתשתית המטרה באמצעות תקיפת תשתית אחרת

המקושרת אליה: ייתכן שדווקא במערכותיה של התשתית המקושרת יימצאו נקודות תורפה שיאפשרו תקיפה קלה ונוחה יותר.

המתודולוגיה התיאורטית המשמשת לבחינת התלות בין תשתיות חיוניות מוצגת באיור מספר 1, הלקוח מתוך מחקרם של ג'ילֶט, פישר, פירנבום וויטפילד.[8] האיור מדגים את הקשרים ואת התלות ההדדית בין התשתיות החיוניות, כאשר במרכז ממוקמת תשתית החשמל הקשורה לכל האחרות, וכולן תלויות בה להפעלתן התקינה.

איור 1: תשתיות חיוניות קשורות ותלויות זו בזו בארצות הברית



המקור: Gillette, J., Fisher, R., Peerenboom, J. and Whitfield, R. (2006). *Analyzing Water/Wastewater Infrastructure Interdependencies*. Lemont, Illinois: Infrastructure Assurance Center – ANL (Argonne National Laboratory): April 01, 2006.

תחילת העיסוק בתחום התלות בין התשתיות

נושא התלות ההדדית בין תשתיות חיוניות בארצות הברית מוזכר לראשונה בצו הנשיאותי מספר 63 משנת 1998, העוסק בהגנה על תשתיות.[9] שני אירועים השפיעו על פרסום צו זה: הפיגוע בבניין הממשל באוקלהומה ב־19 באפריל 1995 ופעילותו של צוות המשימה המדעי בנושא לוחמת מידע בשנת 1996.

הצו הנשיאותי מספר 63 מצהיר לראשונה כי הביטחון הלאומי והכלכלי של האומה האמריקאית תלוי בתשתיות החיוניות ובמערכות המידע התומכות בפעולתן התקינה. כדי להבטיח את אמינותן והגנתן של תשתיות ומערכות אלו,

הוקמו ועדות לכל מגזר תשתית, בעוד שהרשות הפדרלית המתאימה יועדה לחקור בעיות רלוונטיות לכל מגזר. בפועל, פעילותן של הוועדות המגזריות התמקדה בהגנת מערכות המידע מפני חדירה זדונית – כלומר, מתקפות מחשב – אשר עלולה לגרום לכשל בתשתיות החיוניות.

ניתן לחלק באופן גס את התשתיות החיוניות לשני אשכולות:

א. תשתיות שבסיס פעילותן נשען על מערכות של טכנולוגיית מידע (IT) בלבד, דוגמת מרבית התשתיות הפיננסיות.

ב. תשתיות המופעלות על ידי מערכות "סקאדה". אלו הן מערכות שליטה, בקרה וניהול ייעודיות, המאפיינות תשתיות לאומיות קריטיות, כגון חשמל, מים, גז, דלק, תקשורת ותחבורה. המידע במערכות אלו נשלח מהבַּקרים הפזורים בשטח אל מרכז השליטה, וממנו למערכות הביצוע. המערכות נעזרות בחיישנים המחווים את מצב המערכת בזמן אמת, לצורך בקרה ויישום של שינויים תפעוליים. כך, לדוגמה, החיישנים בוחנים בזמן אמת את כמות ונפח החומר העוברים בצנרת שמובילה את אותו החומר מהמכל למתקן העושה בו שימוש.

מודל מתאים לתיאור התנהגותן של תשתיות חיוניות ושל התלות ההדדית ביניהן מתבסס על הגדרת מערכות תשתית כ"מערכות מורכבות־מסתגלות" (Complex Adaptive Systems – CAS). המונח CAS נטבע במכון הבין־תחומי בסנטה פֶּה על ידי ג'ון הולנד (John Holland), הפיזיקאי מוריי גל־מן (Murray Gell-Mann) ואחרים בשנת 1994. מערכות מורכבות־מסתגלות נחשבות למורכבות משום שהן מגוונות וכוללות מספר גדול של רכיבים המקושרים ביניהם; הן גם מסתגלות מכיוון שיכולותיהם של רכיבים וחוקי ההחלטות שלהם משתנים על פני הזמן, כמענה לתגובות הדדיות לרכיבים אחרים ולהתערבויות חיצוניות. דוגמאות נוספות למערכות מורכבות־מסתגלות הן שוק המניות, מושבות חרקים ונמלים, מערכות אקלים, המוח האנושי ומערכת החיסון.

מסגרת כללית לתיאור תלות הדדית בין תשתיות

בשנת 2001 הציע סטיבן רינאלדי, ששימש באותה עת ראש ענף מודרניזציה וטכנולוגיה במטה חיל האוויר האמריקאי, מסגרת כללית לתיאור תלות הדדית בין תשתיות. במחקר, שבו השתתפו חוקרים נוספים, זוהו מערכות תשתית כ־CAS והוצגו שישה מישורי התייחסות שעל פיהם ניתן לספק נתונים על התלות ההדדית בין תשתיות (להלן – טבלה 1). הנושא הוצג במסמך, המהווה מאז את בסיס הפעילות המחקרית־תיאורטית והמעשית־יישומית בתחום זה.[10]

טבלה 1: שישה מישורי התייחסות הנוגעים לתלות בין תשתיות

סוג התלות	סוג הכשל	מאפיינים תשתיתיים
פיזית גיאוגרפית קישור מִחשובי לוגית (Logical)	משותף (Common Cause) מסלים (Escalating) מדורג (Cascading)	מרחבי (Spatial): פנים תשתיתי פריסה גיאוגרפית טווחי זמן (Temporal Range) מרכיב תפעולי שיקולים ארגוניים
מצב תפעולי (של תשתית)	השפעות סביבתיות	צימוד והתנהגות תגובתית
רגיל מאומץ/משובש בתיקון/ בהתאוששות	מדיניות ציבורית חקיקה ורגולציה גורמים עסקיים־כלכליים בריאות הציבור ובטיחות גורמים פוליטיים וחברתיים טכנולוגיה ואבטחת מידע	עוצמת הצימוד: הדוק / רופף סדר הצימוד: ישיר / עקיף מורכבות הצימוד: ליניארי / מורכב

על פי המסמך, מישור ההתייחסות הראשון שיכול לסמן תלות הדדית בין תשתיות הוא סוג התלות. תלות הדדית מוגדרת כקשר דו־כיווני בין תשתיות, שדרכו או באמצעותו מושפע מצבה של כל אחת מהתשתיות ממצבה של האחרת. הדו־כיווניות עשויה להיות רב־ערוצית, דהיינו תשתית אחת תלויה בתשתית שנייה בערוץ מסוים, ואילו השנייה תלויה בראשונה בערוץ אחר. תלות בין שתי תשתיות מוגדרת כקשר חד־כיווני כאשר מצבה של התשתית האחת משפיע על מצבה של התשתית האחרת אך לא להיפך. לדוגמה, מערכת תקשורת תלויה בתשתית החשמל לצורך אספקת החשמל לפעילות רכיביה, אך ייתכן שתשתית החשמל לא תהיה תלויה בפעילות מערכת התקשורת.

מחברי המסמך מבחינים בארבעה סוגים של תלות:

א. **פיזית** – שתי תשתיות תלויות פיזית, כאשר מצבה של כל אחת משתיהן תלוי בתוצר פיזי של השנייה. במצב זה, תוצר פיזי של התשתית האחת הוא קֶלט פיזי של התשתית השנייה. לדוגמה, תחנת כוח לייצור חשמל, המופעלת בפחם, מספקת את הכוח לרשת רכבות המשנעת את הפחם לתחנת הכוח.

ב. **גיאוגרפית** – תשתיות תלויות זו בזו מבחינה גיאוגרפית, אם אירוע סביבתי מקומי יכול לגרום לשינוי במצבה של כל אחת מהן.

ג. **קישור מְחשובי** – זוהי תלות הנובעת ממצב של תשתית המותנה במידע המשודר דרך תשתית המידע או התקשורת. לדוגמה, ייצור החשמל בתשתית חשמל מותנה, בין היתר, במידע המועבר בתשתית המידע על צריכת החשמל של הצרכנים.

ד. **תלות לוגית** – שתי תשתיות תלויות לוגית כאשר מצבה של האחת תלוי במצבה של האחרת באמצעות מנגנון כלשהו שאינו קשר פיזי, גיאוגרפי או מחשובי. תלות מעין זו נוצרת בעיקר באמצעות תהליכי קבלת החלטות של הגורם האנושי – למשל, באמצעות מהלכים פוליטיים, חוקיים, רגולטוריים או עסקיים (כגון מיזוגים).

מישור ההתייחסות השני שיכול לסמן תלות הדדית בין תשתיות הוא **סוג הכשל**. שלושה סוגי כשלים יכולים להשפיע על תשתיות התלויות הדדית:

א. **כשל משותף (Common Cause Failure)** – שיבוש בשתי תשתיות או יותר, המושפעות בו־זמנית כתוצאה מגורם משותף. לדוגמה, כשלים בתשתיות שונות עקב פגעי מזג אוויר.

ב. **כשל מסלים (Failure Escalating)** – כשל בתשתית אחת מעצים שיבוש בלתי תלוי בתשתית אחרת. לדוגמה, זמן התאוששות לתיקון כשל בתשתית שבה התקלקל רכיב עולה, מאחר שתשתית אחרת, למשל תחבורה, אינה זמינה, ועל כן מתעכב משלוח חלקי החילוף.

ג. **כשל מדורג (Cascading Failure)** – שיבוש בתשתית אחת יגרום לשיבוש בתשתית אחרת או בתשתיות אחרות. הדוגמה הבולטת ביותר היא אירוע העלטה באוגוסט 2003 בארצות הברית ובקנדה, כאשר כשל באספקת החשמל גרר הפסקות בתקשורת ובאספקת המים, גרם לעצירת התעבורה האווירית ועוד.

מישור ההתייחסות השלישי שיכול לסמן תלות הדדית בין תשתיות הוא **המאפיינים התשתיתיים**. טבלה מספר 1 מבחינה בארבעה מאפיינים עיקריים:

א. **מאפיין מרחבי (Spatial)**, הכולל שני היבטים: מבנה פנימי של התשתית עצמה ופריסתה הגיאוגרפית. במבנה הפנימי של התשתית החיונית עצמה מבחינים בכמה דרגות של יחידות: חלק, שהוא הרכיב הקטן ביותר שאפשר לאפיין כשמנתחים את המערכת; יחידה, שהיא אוסף של חלקים הקשורים פונקציונלית, למשל גנרטור; תת־מערכת, שהיא מערך של יחידות, למשל יחידת קירור משנית; מערכת, שהיא קיבוץ של תת־מערכות, למשל תחנת כוח. אוסף שלם של מערכות דומות הוא התשתית: כל הגנרטורים, יחידות הקירור ותחנות הכוח, בצירוף חלקים, יחידות, תת־מערכות ומערכות נוספים, יוצרים את

תשתית החשמל. תשתית תלויה הדדית (Interdependent Infrastructure) היא המארג המקושר של תשתיות וסביבה. גם פריסתה הגיאוגרפית של התשתית יכולה להתקיים בכמה דרגות: עירונית – למשל, אספקת מים; אזורית – למשל, מערכות חשמל; לאומית – למשל, מערכות תחבורה; בין־לאומית – למשל, מערכות תקשורת ומערכות פיננסיות.

ב. **מאפיין טווחי זמן (Temporal Range)**. בתפעול תשתיות קיים מנעד עצום של טווחי זמן, הנע מחלקי שניות (למשל, בתפעול מערכות חשמל), דרך שעות (במערכות מים, בגז ובתעבורה) ועד שנים (למשל, שדרוג תשתיות והרחבת קיבולת). להיבט זה יש קשר למאפיין עוצמת הצימוד (הדוק או רופף, כפי שיוסבר בהמשך) בין תשתיות, המשפיעה על רלוונטיות הניתוח. לדוגמה, תהליכים מהירים, כגון תלות הדדית מְחשובית שטווחי הזמן שלה נעים משניות ועד שעות, יכולים להיות מכריעים בניתוח התקדמות של כשל פתאומי ברשת החשמל. הדבר נכון בעיקר כאשר קיימת מעורבות של מערכות "סקאדה" ומערכות ניהול אנרגיה (EMS). תהליכים איטיים יותר, כגון העברת פחם באמצעות רכבות לתחנות כוח (סדר גודל של שבועות), חקיקת חוקי אנרגיה חדשים (יכולה להימשך שנים) או בנייתן של תחנות כוח חדשות (עשויה להשתרע על פני שנים עד עשורים), אינם רלוונטיים לניתוח המתייחס לטווח זמן של ימים בודדים.

ג. **מאפיין המרכיב התפעולי** משפיע על תגובת התשתיות, כאשר הן פועלות במאמץ או תחת הפרעה. המרכיבים התפעוליים קשורים קשר הדוק לאבטחה ולסיכונים. הם כוללים נהלי תפעול, הדרכת מפעילים, מערכות גיבוי ויתירות מערכות, מעקפים בחירום, תוכניות להמשכיות ותוכניות למדיניות אבטחה, כולל יישום ואכיפה.

ד. **מאפיין השיקולים הארגוניים** הוא גורם חשוב בהתנהגות התשתית, ונכללים בו השפעות של גלובליזציה, בעלות בין־לאומית, רגולציה, בעלות ממשלתית כנגד בעלות פרטית, מדיניות והנעה ארגוניות והסביבה הרגולטורית. היבטים ארגוניים אלה עשויים להיות גורמי מפתח בקביעת המאפיינים התפעוליים של התשתיות, ויש להם השלכות ניכרות בתחום האבטחה ומניעת סיכונים.

מישור ההתייחסות הרביעי שיכול לסמן תלות הדדית בין תשתיות הוא **מצבה התפעולי של התשתית**. מדובר ברצף התנהגויות שונות בעת מצבי תפעול שגרתיים, הנעים ממצבים של פעילות שיא למצבים של שפל, בעתות לחץ או כאשר מתגלים שיבושים, או בעת ביצוע תיקונים ושיפוצים. מצב הפעילות של יחידה, תת־מערכת או מערכת בעת כשל משפיע על היקף השיבוש, על משכו ועל הפגיעה באספקת השירות שמציעה התשתית. כך, למשל, השפעת אירועים שיתרחשו בעת דרישות

שיא לחשמל (או גז, או מים, או טלפוניה, או בעת תעבורה כבדה) תהיה שונה מהשפעת אירועים זהים שיתרחשו כאשר הצריכה נמצאת בשפל.

מישור ההתייחסות החמישי לבחינת תלות הדדית בין תשתיות הוא **השפעות סביבתיות**. תשתיות פועלות בסביבה המתוארת לא רק על ידי קלטים, פלטים ומצבי תפעול, אלא גם בסביבת מאפיינים של תשתיות אחרות ושל גורמים כלליים נוספים. סביבת התשתית היא המסגרת שבה בעלי התשתית ומפעיליה מציבים יעדים, יוצרים ערך למערכות, מדמים ומנתחים את פעילותן ומקבלים החלטות המשפיעות על מבנה התשתיות ועל פעולתן. טבלה מספר 1 מציינת כמה קבוצות של גורמים כאלה:

א. **מדיניות ציבורית**. המדובר במדיניות אנרגיה פדרלית, במדיניות אבטחה, במדיניות כלכלית, במדיניות התגובה לאסונות ובמדיניות המגדירה את תחומי הסמכות השיפוטית. כדוגמה למדיניות כזו אפשר לציין את החלטת הוועדה הפדרלית לתקשורת של ארצות הברית (Federal Communications Commission – FCC) שלא להסדיר את שירותי ספקי האינטרנט – דבר שהשפיע באופן מהותי על עיצוב תשתיות התקשורת ועל צמיחתן.[11] החלטות בעניין השקעות ממשלתיות הן גורם חשוב נוסף של מדיניות ציבורית המשפיעה על הסביבה שבה פועלות תשתיות. דוגמאות לכך הן השקעות פדרליות בטכנולוגיות ביטחוניות, ברשתות מחשבים ובתקשורת לווינית, אשר על בסיסן התפתחו תשתיות מסחריות מקיפות.

ב. **גורמי חקיקה ורגולציה** משתייכים אף הם לתחום המדיניות הציבורית, אך בשל חשיבותם הרבה הם זוכים להתייחסות נפרדת. היבטים חוקיים ורגולטוריים משפיעים ישירות על פעילותן של תשתיות. תשתיות המוסדרות ברגולציה פועלות תחת מערכת אילוצים הדוקה יותר מאשר תשתיות המשוחררות כליל מרגולציה. דוגמה לכך הם חוקים המשיתים אחריות משפטית על חשיפת מידע פרטי, רפואי ובנקאי. חוקים אחרים עשויים להשפיע על מבנה התשתית – למשל, חקיקה המחייבת שירותי תקשורת.

ג. **גורמים עסקיים־כלכליים**. הזדמנויות וסיכונים עסקיים־כלכליים הם כוחות חשובים המעצבים את הסביבה שבה פועלות תשתיות. בעלי התשתיות מחליטים על פי כוחות אלה החלטות עסקיות ומבניות המשפיעות על מאפייני הפעילות. פיתוחים מטכנולוגיית המידע, פיקוח ממשלתי או הסרתו וכן מיזוגים הם שלושה גורמים שיש להם השפעה גדולה על המאפיינים העסקיים והכלכליים של סביבת התשתיות.

ד. **בריאות הציבור ובטיחות**. חקיקה ורגולציה שמכוונת להגנה על חיי אדם, רכוש, בריאות הציבור ובטיחות משפיעות באופן ישיר על פעילותן של תשתיות ועל התלות ההדדית ביניהן. לדוגמה, רגולציה להגנת הסביבה בקליפורניה קובעת

תקנים מחמירים נגד פליטת חומרים מזהמים מתחנות כוח, זיהום אוויר ותופעות אחרות המשפיעות על הבריאות. רגולציה זו משפיעה ישירות על החלטות תפעוליות, על בניית תחנות כוח חדשות תוך שימוש בטכנולוגיות חדישות, על הבחירה במערכות "סקאדה" ובמערכות אלקטרוניות אחרות ועל סוגי הדלק שבהם ישתמשו. החלטות אלו משפיעות על התלות ההדדית שנוצרת בין התשתיות.

ה. **גורמים פוליטיים וחברתיים** הם אלה המניעים שווקים ובחירות ומהווים בסיס לקביעת רמת הנחיצות של חוקים ושל רגולציות, רמת אספקת השירות, היקף ההגנות ורמת יישומן. גם כוחות ואינטרסים חברתיים ופוליטיים בין־לאומיים מעצבים את סביבת התשתית, שכן רבות מהתשתיות הפכו לבין־לאומיות. למשל, תשתית החשמל האמריקאית מאוחדת היום עם תשתית החשמל הקנדית, וגם תשתיות נוספות הן בין־לאומיות, כמו תשתיות תקשורת, דלק וגז. נושאים פוליטיים משפיעים על תהליכים בתשתיות ובסביבתן, כמו הפקת חשמל ממים בצפון־מערב האוקיינוס השקט, בעלות לא אמריקאית על תשתיות התקשורת האמריקאית ועוד.

ו. **טכנולוגיה ואבטחת מידע**. כשלי אבטחה בתשתית אחת מעלים את רמת הסיכון ופוגעים באבטחה בתשתיות אחרות הנתמכות על ידה. כך, לדוגמה, אם תבוצע תקיפה מוצלחת על מערכת ה"סקאדה" של רשת החשמל המקומית המניעה מערכת מים עירונית, מערכת אספקת המים עלולה לסבול מהפרעות. אבטחת מערכת המים היא פועל יוצא של רמת האבטחה במערכת אספקת החשמל, וגם הסיכון לשיבוש או לכשל הוא פועל יוצא של רמה זאת.

מישור ההתייחסות השישי לבחינת תלות הדדית בין תשתיות הוא **צימוד (Coupling) והתנהגות תגובתית**. בנושא זה מבחינים רינאלדי ועמיתיו בשלושה נושאים שאליהם יש להתייחס:

א. **עוצמת הצימוד – הדוק או רופף**. צימוד הדוק מתייחס לתשתיות התלויות תלות גדולה זו בזו. הפרעה בתשתית אחת מקושרת באופן מידי להפרעה בתשתית האחרת. דוגמה למצב כזה היא תחנת כוח המונעת בגז טבעי והצינור המזרים את הגז הטבעי. אם לא קיים מאגר גז מקומי ואם התחנה לא יכולה לעבור להשתמש במקור דלק חלופי, הצימוד הדוק במיוחד. במצב זה, הפרעה באספקת הגז תגרום מיד להפרעה בייצור החשמל. צימוד רופף מתקיים כשהתשתיות הן עצמאיות יחסית, ומצבה של האחת כמעט אינו משפיע על מצבה של האחרת. דוגמה לכך היא תחנת כוח המונעת בפחם, שבדרך כלל יש במחסניה די פחם להפעלתה למשך חודשיים־שלושה, ורשת הרכבות

שבאמצעותה מסופק הפחם. הפרעה זמנית לאספקת הפחם אינה משפיעה באופן מידי על תפקודה של תחנת הכוח.

ב. **סדר הצימוד – ישיר או עקיף**. צימוד ישיר מתקיים כשתשתית אחת מחוברת ישירות לתשתית שנייה. צימוד עקיף מתקיים כאשר התשתית השנייה מחוברת לתשתית שלישית. במצב זה התשתית הראשונה מחוברת באמצעות התשתית השנייה לתשתית השלישית, ועל כן התשתית השלישית מחוברת לתשתית הראשונה בצימוד עקיף. דוגמה לצימוד ישיר היא הפרעה באספקת חשמל שתגרום לבעיות בייצור גז טבעי. בהמשך השרשרת ייפגעו מפעלים הזקוקים לגז טבעי לפעולתם. זהו הצימוד העקיף שבין אספקת החשמל לבין המפעלים הללו.

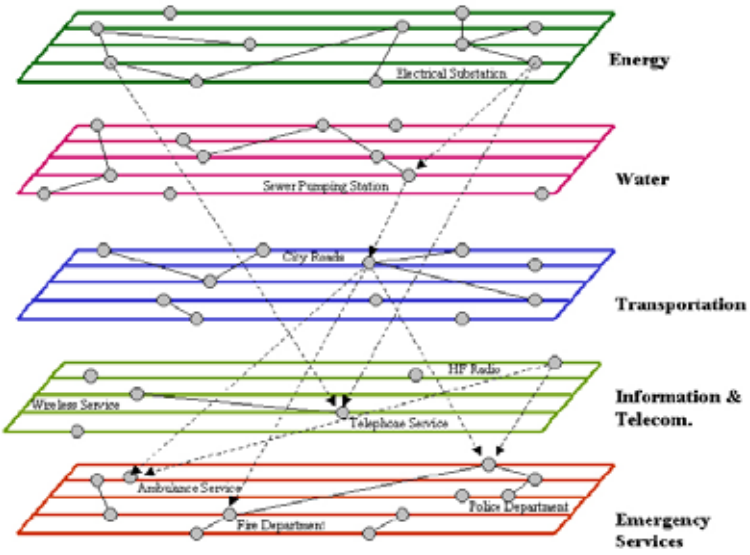
ג. **מורכבות הצימוד – ליניארי או מורכב**. פעילות הדדית ליניארית היא חלק מרצף פעולות הייצור או התחזוקה. עם זאת, פעולות אלו, שהן מוכרות וידועות, עשויות להתרחש באופן בלתי צפוי. פעילות הדדית מורכבת היא פעילות שאינה חלק מהרצף התפעולי, או שהיא בלתי מתוכננת ובלתי צפויה, אינה גלויה לעין ואינה מובנת מיד. כך, לדוגמה, כאשר תשתית לאספקת גז טבעי נבחנת במנותק מתשתיות אחרות, ניתן להתייחס אליה לכאורה כאל מערכת ליניארית: גז זורם ממקור מסוים, עובר למפעל לייצוב הגז, משם הוא זורם דרך תחנות דחיסה ושערים רבים, לאתר הצרכן. אם תחנת ייצור החשמל משתמשת בגז הטבעי כמקור דלק, והחשמל משמש להפעלת תחנות הייצוב ודחיסת הגז, אזי הצימוד בין התשתיות גז־חשמל הוא מורכב ולא ליניארי.

דוגמה למערכת תשתיות התלויות זו בזו ומשפיעות זו על זו אפשר לראות באיור מספר 2.

האיור מראה כיצד תשתיות במרחב עירוני קשורות האחת לאחרת, תלויות הדדית ומושפעות זו מזו. על פי המודגם באיור, שירותי החירום העירוניים, דוגמת משטרה, מכבי אש ואמבולנסים, תלויים בתשתיות התקשורת והתחבורה, ואלו תלויות ישירות בתשתיות האנרגיה. קיימת גם תלות בין תשתית התחבורה לתשתית המים.

בטבלה מספר 2 מוצגת עוצמת התלות בין התשתיות השונות בשלוש רמות – גבוהה, בינונית ונמוכה. כך, למשל, לתעשיית המזון תלות גבוהה בתשתיות החשמל, המים וטיהור השפכים ותלות נמוכה בתשתיות הגז הטבעי. לשירותי הבריאות תלות גבוהה באספקת החשמל והמים, ולתשתית החשמל תלות גבוהה באספקת הגז הטבעי.

איור 2: התלות ההדדית בין תשתיות עירוניות[12]



המקור: Pederson, P., Dudenhoeffer, D., Hartley, S., and Permann, M. (2006). *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Idaho National Laboratory (INL): August 2006

טבלה 2: עוצמת התלות בין תשתיות[13]

המגזר		אנרגיה ויישומים					שירותים	
	התשתית	חשמל	מי שתייה	טיהור שפכים	גז טבעי	זיקוק נפט	בתי חולים ושירותי בריאות	תעשיית המזון
אנרגיה ויישומים	חשמל		ג		ג	ב		
	מי שתיה	ג				ב		
	טיהור שפכים	ב	נ			נ		
	גז טבעי	נ				נ		
	זיקוק נפט	ג	נ					
שירותים	בתי חולים ושירותי בריאות	ג	ג	נ	ב	ג		ג
	תעשיית המזון	ג	ג	ג	נ	ב	נ	

ג – גבוהה ב – בינונית נ – נמוכה

פועל יוצא מכל האמור עד כאן הוא שפגיעה ישירה בתשתית חיונית עלולה לפגוע בעקיפין, ואולי אף ישירות, בתשתיות נוספות במדינה המותקפת, ואולי גם במדינות נוספות, ובהן מדינתו של התוקף עצמו. פגיעות אלו עלולות לגרום גם לביצוע פשעי מלחמה. כך, למשל:

א. תקיפת תשתית הולכַת גז טבעי של מדינה עלולה להשפיע על יכולת ייצור האנרגיה גם במדינות נוספות המחוברות לתשתית זו, אך אינן בהכרח צד לסכסוך. הפגיעה בייצור האנרגיה יכולה לגרום בהמשך לפגיעות בשירותים ובתשתיות חיוניות במגזר האנרגיה ובמגזרים נוספים, עד כדי פגיעה בחיי אדם. זאת, בשל שיבושים בבתי חולים, ובעיקר בחדרי מיון, פגיעה בפעילות רמזורים בצמתים, הפרעות בפעילות מפעלים חיוניים וכדומה.

ב. תקיפת מערכת המשמשת לניהול תשתית מחשב של מערכת בנקאות עלולה לשבש תהליכים והעברות כספיות, שמצָדם יגרמו נזק ישיר לחברות בין־לאומיות. בין חברות כאלו עשויות להימצא חברות ממדינתו של התוקף.

ג. תקיפת תשתיות המפעילות נמל גדול – דוגמת מערכות להעמסת מטענים על אוניות מטען או מכליות נפט – עלולה להשפיע על כלל התעבורה הימית העולמית: כניסתן של ספינות לנמל תעוכב, ובשל כך ייפגעו לוחות הזמנים של קווי ספנות ברחבי העולם. גם נמלים השייכים לתוקף עשויים להיפגע. הדבר כרוך באובדן הכנסות כספיות ובפגיעה כלכלית גדולה.

ד. תקיפה המכוּונת לשבש פעולתם של רמזורים בצמתי מפתח, במטרה לעכב תנועת כוחות לחזית, עלולה לגרור עיכובים ושיבושים גם בתנועת אמבולנסים וכוחות חירום והצלה. תקיפה לשיבוש פעולתן של רכבות עלולה לפגוע גם בתנועת סחורות ומזון. במקרים מסוימים עלולה תקיפה כזאת לגרום לירידת רכבות מהמסילה, תוך סיכון חיי אדם.

בנוסף לנאמר לעיל, ניהול מערכה קיברנטית עשוי להיות מושפע מאוד מהתלות ומהקשרים בין התשתיות. בעלות בין־לאומית של תאגיד על תשתית משפיעה על המגן ועל התוקף גם יחד. גורמי הגנה עשויים לנצל את העובדה שהתשתית שעליה הם מגנים נמצאת בבעלות תאגיד בין־לאומי שבשליטתו גם תשתיות במדינת היריב. אותם גורמים יכולים להשפיע על היריב לא לתקוף, כדי שתשתיותיו־הוא לא תיפגענה כתוצאה מהתקיפה. גורמי תקיפה, מצדם, עשויים למצוא תועלת רבה בבעלות בין־לאומית כזו, שכן הם יוכלו לנצל אותה כדי לאסוף מידע על התשתית שיבקשו לתקוף, ואולי גם כדי להחדיר חומרה או תוכנה לשימוש עתידי במהלך תקיפה.

השפעת התלות בין התשתיות על מאפייני הפעילות הקיברנטית האמריקאית

המאפיינים של מרכיבי התשתיות והתלות ההדדית ביניהן משפיעים על הסתגלותה של התשתית ועל גמישותה. מודל CAS של מערכת מורכבת־מסתגלת מאפיין מערכת על פי יכולתה ללמוד מניסיון העבר ולהתאים עצמה לצפי העתידי. גורמים רבים תורמים לסתגלנות של מערכת: זמינות, מספר החלופות לתהליכים או למוצרים קריטיים, תוכניות המשכיות לעת חירום, מערכות גיבוי, הדרכת כוח האדם התפעולי ויצירתיות הגורם האנושי במצבי אסון. גורמים אחרים עלולים להפוך תשתית לבלתי גמישה: רגולציה וחקיקה מגבילה, היבטים חברתיים, מדיניות ארגונית וטופולוגיות רשת קבועות[14]. לאוסף של רכיבים גמישים יש סיכוי גדול יותר להגיב טוב יותר להפרעות ולהמשיך לספק מצרכים ושירותים חיוניים.

דרך הפעולה האמריקאית גורסת קיומה של מסגרת ועטיפה קיברנטית לכל תרחיש צבאי. השאיפה היא להגיע ליכולת נטרול של מערכות ההגנה של הצד היריב טרם פתיחת הלחימה, ובמקביל לספק אבטחה למערכות המידע והתקשורת של הכוחות הלוחמים של ארצות הברית. כך, בצד הפגיעה ביכולותיהן של מערכות השליטה והפיקוד של היריב, ייפגעו גם מרכיבים קריטיים ויכולתו להפעיל את מערכי הלחימה.[15]

הדוקטרינה שהתבססה בארצות הברית מחייבת בנייה וקיום עליונות קיברנטית מלַווה לכל פעילות קרבית, בהתאמה ליכולות היריבים. האסטרטגיה האמריקאית גורסת אחיזה קיברנטית במערכי הפיקוד, השליטה והלוגיסטיקה של היריבים הפוטנציאליים במטרה לנסות להכריע את המערכה עוד טרם החלה, ואם תתפתח – לפגוע במערכים אלה על פי הצורך. לפי התפיסה האמריקאית, אין קינטי בלי קיברנטי. הווה אומר, פעולות שבהן ייעשה שימוש ביכולות קונוונציונליות (קרי, אמל"ח קינטי) יִלָוו תמיד במעטפת מבצעית קיברנטית. פעולות מלחמתיות קינטיות, שנועדו להשיג מטרות בדרך הטובה והיעילה ביותר, אינן עומדות עוד בפני עצמן, אלא נדרשת מעטפת קיברנטית מלַווה להן. בנוסף לכך, כל פעילות תקיפה במרחב הקיברנטי תלָווה בפעילות איסוף מקדימה – גם היא במרחב הקיברנטי.

כדי לקיים אסטרטגיה זו, הקימו הזרועות הלוחמות של ארצות הברית מערכי פעולה למרחב הקיברנטי, שהם בעלי יכולות הגנה ותקיפה הנסמכים על יכולות פיקוד הסייבר (ולמעשה, על יכולותיה המופלגות של הסוכנות לביטחון לאומי). משימותיהם של מערכים אלה כוללות אבטחת המרחב הקיברנטי שבו פועלות המערכות הצבאיות ותמיכה טכנולוגית ביחידות הקינטיות, וכן **הכרעת כל יריב פוטנציאלי ו"שמירה על העליונות האמריקאית במרחב הקיברנטי"[16], תוך תקיפת מערכי היריב במרחב זה**. ליכולת ההגנה תפקיד מכריע בהתמודדות ובניצחון בסביבה אסימטרית, דוגמת זו שאותה חווים האמריקאים מול יריביהם במרחב

הקיברנטי. משום כך קיים צורך אקוטי ליצור איזון בין יכולות התקפה והכרעה לבין יכולות הרתעה והגנה.

באוקטובר 2012 חתם הנשיא אובמה על הצו הנשיאותי מספר 20, המסווג סודי ביותר, אשר מתווה את התשתית החוקית ואת הנהלים שבבסיס המדיניות הקיברנטית של ארצות הברית. הצו כולל הנחיות ליישום אמות מידה לפעולות של כלל גורמי הממשל האמריקאי בהתמודדותם עם איומים במרחב הקיברנטי. מוגדרים בו מונחי היסוד הרלוונטיים למרחב הקיברנטי, דוגמת מִבצעי תקיפה והגנה, הגנה על רשתות, פעילות עוינת, פעולות השפעה ואיסוף במרחב. כמו כן מודגש בו הצורך לפתח כלים קיברנטיים ולהשתמש בהם כחלק אינטגרלי מעוצמתה ומביטחונה הלאומי של ארצות הברית מול יריביה.

המדליף אדוארד סנואדן חשף כי הנשיא אובמה הִנחה בצו הנשיאותי מספר 20 את גורמי הממשל האמריקאי לבחון, בין היתר, את השפעת פעולותיהם על גורמים העלולים להיפגע מהן.[17] לפי סנואדן, פעילות שעלולה לגרום לפגיעה בחיי אדם, לפגיעה משמעותית באינטרסים אמריקאיים או לנזק משמעותי לרכוש, מחייבת אישור נשיאותי.

מניסוח הצו הנשיאותי ברור כי כותביו מודעים לאפשרויות הפגיעה ההדדית כתוצאה מהתלות בין התשתיות. בהקשר זה מגדיר הצו[18]:

א. פעולות יבוצעו בהתאם לדיני המלחמה.

ב. פעולות שעלולות להיות בעלות השפעות קיברנטיות בתחומי ארצות הברית מחייבות אישור נשיאותי. יש לעשות מאמץ לאתר כל גורם העלול להיות מושפע מן הפעולה – הן ברחבי ארצות הברית והן בקרב גורמי היריב.

ג. פעולות שעלולות לגרום להשלכות משמעותיות (ובמשתמע, גם על תשתיות אמריקאיות וזרות) מחייבות אישור נשיאותי בשגרה (בחירום מתקיים תהליך אחר). פעולות סייבר, אשר יבוצעו בתגובה לפעולות של היריב, יש לבצע באופן שלא יגרום להשלכות משמעותיות.

ד. בעת הדיון על ביצוע הפעולה יש לשקול את ההשפעה שתהיה לה על אינטרסים אמריקאיים, בכלל זה פגיעה ברשתות ותשתיות תקשורת. יש למפות תגובות והשלכות אפשריות של פעולות בסייבר על אינטרסים אמריקאיים ולעשות הכנות מתאימות טרם ביצוע הפעולה.

ב־27 במאי 2013 פורסם כי בכוונת המטות המשולבים של ארצות הברית להקנות למפקדי הכוחות המזוינים סמכויות שיאפשרו להם להשתמש באמל"ח קיברנטי התקפי בתגובה לאיומים קיברנטיים, וזאת גם ללא אישור המועצה לביטחון לאומי (כפי שנדרש עד אז). נהלים אלה סוכמו למעשה עוד בשנת 2010, אולם אישורם

התעכב בשל מחלוקת משפטית באשר לסמכויות ההפעלה ועוצמת המענה לתקיפות קיברנטיות. רק אחרי עבודת מטה ממושכת גובשו הסכמות בנושא זה.[19]

יכולותיה הטכנולוגיות המופלגות של המעצמה ארצות הברית נסמכות, בין היתר, על העובדה שרוב המערכות המפעילות את המרחב הקיברנטי נשענות על פעילותם של תאגידים, שחלקם הגדול נמצא בבעלות אמריקאית, ולמרבית האחרים יש זיקה לארצות הברית. תאגידים אלה מאפשרים לארצות הברית שליטה ודומיננטיות מובהקות בכל תחומי המרחב הקיברנטי, בכלל זה אפשרות לפגוע ביריבים פוטנציאליים ואף להרתיע אותם מפני פעילות שתגרור פגיעה קשה בהם.

ניהול מערכה קיברנטית מעלה סוגיות חדשות בעולם האסטרטגיה והביטחון. כך, למשל:

א. מפקדים וגורמי פיקוד חייבים להכיר היטב ולהבין את המערכות ואת הטכנולוגיות המתחדשות לעתים מזומנות. הכרת הטכנולוגיה מאפשרת להבין את המשמעויות האפשריות של אירועי לוחמה קיברנטית.

ב. האמל"ח הקיברנטי הוא כלי לחימה זול, וגם הכשרת התוקפים אינה דורשת השקעות ניכרות. עלויות נמוכות אלו מאפשרות גם לגורמי טרור ולמדינות מעוטות אמצעים להשתתף במערכה הקיברנטית.

ג. המערכה מתנהלת על גבי תשתיות חיוניות ועל גבי מערכות מידע המשמשות במרבית המקרים גם את האוכלוסייה האזרחית. כאשר התשתיות ומערכות המידע הן החזית, טכנאֵי המערכות הופכים ללוחמים, והם אלה אשר עשויים להכריע את המערכה.

ד. במקרה של פגיעה בתשתית, הקשרים בין התשתיות ומעורבותו של השוק האזרחי בניהול מערכות מידע ותשתיות עלולים לגרום לתגובת שרשרת נרחבת.

ה. היעדר חקיקה מסדירה ואמנה בין־לאומית בנושא הלחימה הקיברנטית מגביר את הבעייתיות של ההיתרים והאיסורים במערכה זו. בעיקר קיימת אי־בהירות באשר לפגיעה בתשתיות אזרחיות.

עולם מערכות המידע והביטחון השתנה מאוד בעשורים האחרונים. ארצות הברית הפעילה יכולות קיברנטיות מלחמתיות כבר במלחמת המפרץ הראשונה בשנת 1991, וידוע על פעילות קיברנטית חשאית שבוצעה על ידי גורמי מודיעין אמריקאיים שנים קודם לכן. ברור לחלוטין כי לוחמה קיברנטית תהיה חלק מכל מערכה מודרנית ועתידית, וכי לעתים היא תשפיע עליה השפעה דרמטית, עד כדי הכרעת המערכה.

במלחמות עבר פעלו כוחות ארצות הברית באופן אלים ולעתים מבלי לבחול בפגיעה בחפים מפשע. הלוחמה הקיברנטית מאפשרת לכוחות האמריקאיים לפעול באופן מדוד ומתון, תוך ניסיון להימנע מפגיעה בבלתי מעורבים. יתרה מכך,

קובעי המדיניות בארצות הברית יצרו תדמית, לפיה מאפייני התרבות והדמוקרטיה האמריקאיים מציבים רסנים ובלמים כבדים על הפעלת הכוח הקיברנטי במבצעי תקיפה. זה המקום להזכיר כי עד לחשיפה המידע הרב על ידי סנואדן, הממשל האמריקאי דיבר בעיקר על נושא ההגנה מפני תקיפות סייבר, תוך שהוא מאשים בפומבי את סין בביצוע תקיפות סייבר נגדו. המידע שנחשף על ידי סנואדן הראה כי באותה העת שארצות הברית הטיחה האשמות בסין, היא עצמה ביצעה פעולות סייבר התקפיות נגד הממשל הסיני. חשיפה זו הביאה את סין להאשים באופן פומבי את ארצות הברית במה שכינתה "המוסר הכפול" שלה.[20]

בהקשר זה הושמעה גם הטענה בדבר "צביעותה" של ארצות הברית. כך, לדוגמה, הועלתה הטענה כי הפעולות האמריקאיות שנחשפו אינן עולות בקנה אחד עם המדיניות הרשמית של ארצות הברית בתחום הסייבר וכי הממשל האמריקאי יתקשה להצדיק את פעילותו זאת. לפי תפיסה זו, הצביעות היא חלק חשוב במרכיבי "העוצמה הרכה" (Soft Power) שבהם משתמשת ארצות הברית כדי לגרום למדינות אחרות ברחבי העולם לקבל את הלגיטימיות של מעשיה.[21]

התלות הישירה בין התשתיות עשויה לגרום לכך שתקיפת תשתית מידע צבאית תיצור תגובת שרשרת שתפגע בתשתיות אזרחיות. כאמור, תקיפת תשתית קריטית של מדינה עלולה להשפיע על תשתיות ועל יכולות ייצור במדינות נוספות המחוברות לתשתית זו ואינן צד לסכסוך שבמסגרתו בוצעה התקיפה. משום כך, תקיפה כזאת מצדה של ארצות הברית עלולה לגרור ביצוע פשעי מלחמה ואף לפגוע תוך כדי כך באינטרסים אמריקאיים. נראה כי תקיפה של מטרות צבאיות טהורות, כמו מערכות מכ"ם ומערכות נגד מטוסים, או מערכות ליבה של ייצור והפצת נשק לא קונוונציונלי, היא משימה שהוצאתה אל הפועל קלה הרבה יותר.

התלות הקיימת בין התשתיות מחייבת את גורמי התקיפה האמריקאיים המתכננים לפעול מול תשתיות זרות לבחון היטב את הקשרים בין התשתיות שבכוונתם לתקוף ובין תשתיות אחרות – במדינת היעד, בארצות הברית ובמדינות נוספות. הבחינה תאפשר לעתים לפגוע בתשתית המטרה בקלות ובנוחות רבות יותר, באמצעות תקיפת תשתית מקושרת שבמערכותיה יימצאו נקודות תורפה.

כותבי מאמר זה מעריכים כי גורמי התקיפה האמריקאיים יקיימו פעילות איסוף נגד יריבים, ואף יפגעו בגורמי תקיפה שלהם, כאשר הללו יפעלו נגד תשתיות אמריקאיות. תיתכן הפעלה של כלי תקיפה אמריקאיים, שאפקט הפגיעה שלהם בתשתיות של מדינות יריב לא יהיה הרסני. גם תיתכן הפעלה של כלי תקיפה ממוקדי מטרה שיצליחו לדלג על מערכות שאין לארצות הברית כוונה לפגוע בהן, דוגמת פעולתה של התולעת סטוקסנט.

קובעי המדיניות האמריקאיים ימשיכו לשאוף לקידום חקיקה בין־לאומית בנושאי הפעילות במרחב הקיברנטי, או לכל הפחות להסדרה בין־לאומית בסוגיה

זו במסגרת ועידות טאלין (מטעם נאט"ו),[22] או בהסתמך על אמנת בודפשט.[23] קרוב לוודאי שארצות הברית גם תשאף למצוא פתרונות מוסריים לניהול המערכה הקיברנטית באירועים שבהם עלולים להיפגע חיי אדם.

הערות

1 Federation of American Scientists, *National Security Presidential Directives [NSPD] George W. Bush Administration*, http://www.fas.org/irp/offdocs/nspd/index.html; Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare*"*, *The Washington Post*, February 7, 2003.

2 *The National Strategy to Secure Cyberspace*, *President Bush*, Washington, February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

3 Lolita C. Baldor, "Military gets cyberwar guidelines", *The Washington Times*, June 22, 2012, http://www.washingtontimes.com/news/2011/jun/22/military-gets-cyber-war-guidelines

4 Patricia Zengerlensa, "NSA chief warns Chinese cyber attacks could shut U.S. infrastructure", Reuters, November 21, 2014, http://www.reuters.com/article/2014/11/21/us-usa-security-nsa-idUSKCN0J420Q20141121

5 Eric Chabrow, "Obama to Congress: Enact Cybersecurity Laws", *GovInfosecurity,* January 21, 2015, http://www.govinfosecurity.com/obama-to-congress-enact-cybersecurity-laws-a-7816; Nicole Blake Johnson, "Lawmakers Welcome Cybersecurity Talks with Obama", *FedTech*, January 21, 2015, http://www.fedtechmagazine.com/article/2015/01/lawmakers-welcome-cybersecurity-talks-obama

6 Steven M. Rinaldi, James P. Peerenboom and Terrence K. Kelly, "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, December 2001, pp. 11-25, www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

7 *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, U.S.-Canada Power System Outage Task Force, April 2004, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

8 Jerry Gillette, Ronald Fisher, James Peerenboom and Ronald Whitfield, "Analyzing Water/Wastewater Infrastructure Interdependencies," Infrastructure Assurance Center – Argonne National Laboratory (Lemont, Illinois: April 2006), www.dis.anl.gov/pubs/42598.pdf

9 *Presidential Decision Directive/NSC-63: Critical Infrastructure Protection*, The White House, Washington, May 22, 1998, http://fas.org/irp/offdocs/pdd/pdd-63.htm

10 Rinaldi, Peerenboom and Kelly, "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies."

11 *Preserving the Free and Open Internet*, Federal Communications Commission, December 21, 2010, https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf

12 Pederson, P., Dudenhoeffer, D., Hartley, S., and Permann, M. *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research.* Idaho

National Laboratory (INL): August 2006, p.3, http://cipbook.infracritical.com/book3/chapter2/ch2ref2a.pdf

13 Ibid., p.5

14 טיפולוגיית רשת – הכוונה לתצורת הרשת ולהגדרת הקשרים בין הרכיבים שלה. במקרה זה הכוונה לרשת בעלת תצורה קבועה וחסרת יכולת להשתנות על פי תנאים משתנים.

15 הראל מנשרי, **שילוב לוחמה קיברנטית בסוגי לוחמה אחרים, חקר מקרה: ארצות הברית**, חיבור לשם קבלת תואר דוקטור לפילוסופיה, בהנחיית פרופסור שפרה ברוכסון־ארביב, רמת גן, אוניברסיטת בר־אילן, ינואר 2014.

16 GlaGlando, B. LTC(P) (2011, January). *2d Battalion Information Operation Command (LAND) Counter-Cyber Operations*. presented at Cyber Warfare 2011, London, England.

17 "Obama tells intelligence chiefs to draw up cyber target list – full document text", *The Guardian*, June 7, 2013, http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text

18 Presidential Policy Directive/PPD-20, pp.7-10. http://fas.org/irp/offdocs/ppd/ppd-20.pdf

19 Zachary Fryer-Biggs, "Slowed by Debate and Uncertainty, New Rules Green Light Response to Cyber Attacks", *Defense News*, May 27, 2013, http://archive.defensenews.com/article/20130527/DEFREG02/305270014/Slowed-by-Debate-Uncertainty-New-Rules-Green-Light-Response-Cyber-Attacks

20 Jonathan Kaiman, "China reacts furiously to US cyber-espionage charges", *The Guardian*, May 20, 2014, http://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges

21 Henry Farrell and Martha Finnemore, "The End of Hypocrisy – American Foreign Policy in the Age of Leaks", *Foreign Affairs*, November/December 2013, http://www.foreignaffairs.com/articles/140155/henry-farrell-and-martha-finnemore/the-end-of-hypocrisy

22 *Tallinn Manual Process*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, https://ccdcoe.org/tallinn-manual.html

23 Cybercrime Convention Committee, Council of Europe, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp