אכיפת גבולות או חציית גבולות בסייבר: דילמת הריבונות

אלסנדרו גוארינו ואמיליו אזיילו

התפיסה לגבי מרחב הסייבר התפתחה בהדרגה, מהגישות הליברטיניות של שנות התשעים של המאה העשרים ועד המצב הנוכחי, שבו מדינות לאום מבקשות לבסס מחדש את ריבונותן במרחב זה. המאמר בוחן את התפתחות התפיסות לגבי מרחב הסייבר – מהתפיסות האוטופיות שהגיעו לשיאן במה שכונה "הצהרת העצמאות של מרחב הסייבר", ועד לשימת הדגש על הממד הטכנולוגי ומהלכי החקיקה שממשלות נוקטות כיום כדי להגביר את השליטה על מרחב זה. המאמר מתייחס למאמצים שנעשים במערב ובמזרח כאחד לפתור את האתגרים המגוונים, מרובי ההיבטים והמתמשכים שמציב הסייבר. מאמצים אלה נעים מתמיכה במרחב סייבר פתוח ועד לרצון לנטר מקרוב את האיום הגלום בו ואת השחקנים המדינתיים והלא מדינתיים השונים הפועלים במסגרתו. המאמר מתמקד בקשיים הרגולטוריים והטכניים הכרוכים בקביעת גבולות למרחב הסייבר, לרבות ההשלכות שיש לכך על נושאי מדיניות, ומסביר כיצד שחקני סייבר חוצים גבולות באמצעות שימוש בטכניקות שונות, כגון קריפטוגרפיה ו"מקלטי נתונים". המסקנה העיקרית של המאמר היא ש"הבלקניזציה" של מרחב הסייבר אינה רק מציאות קיימת, אלא גם תהליך שקשה לראות כיצד הוא ישנה את כיוונו. הדבר מעלה את השאלה כיצד חברות פתוחות יכולות לאזן בין ריבונות ובין חופש הפרט במרחב הסייבר. ההצעה המועלית במאמר מסתמכת על דוגמאות שבהן הריבונות של מדינות הלאום הינה מוגבלת, והגבולות אינם רלוונטיים, כמו מערכת החוקים הבין־לאומית המסדירה את סוגיית המשאבים הגלובליים.

מילות מפתח: אבטחת סייבר, משילות באינטרנט, יחסים בין־לאומיים, לוחמת סייבר, עימות סייבר, סין, פרטיות

אלסנדרו גוארינו הוא יועץ אסטרטגי בחברת "StudioAG", חברת אבטחת מידע ואבטחת סייבר איטלקית. אמיליו אזיילו הוא מנתח מודיעין סייבר אסטרטגי, המייעץ לארגוני מודיעין צבאיים ואזרחיים של ממשלת ארצות הברית, כמו גם לחברות במגזר הפרטי המספקות מודיעין סייבר.

מבוא

ההתפשטות הכלל־עולמית של תשתית ייחודית להעברת מידע דיגיטלי במהלך העשור האחרון של המאה העשרים, הביאה לשינוי עמוק בכול היבט של החיים והחברה – מאינטראקציות חברתיות ועד לכלכלה הגלובלית. זמינות הגישה לאינטרנט נחשבת כזכות כמעט מובנת מאליה, לפחות במדינות המפותחות. אולם מרחב הסייבר אינו תופעה טבעית, אלא תופעה היסטורית ופוליטית, וככזו הוא נתון להשפעות של ישויות פוליטיות וחברתיות. מבין הישויות הפוליטיות השונות, חשיבות עליונה יש למדינות הלאום.

ממשלת ארצות הברית הייתה גורם מרכזי בפיתוח האינטרנט, מאז תחילתו כפרויקט מחקר בסוכנות לפרויקטים מתקדמים של משרד ההגנה האמריקאי (DARPA). הקהילה הבין־לאומית וחלק מהארגונים העל־לאומיים מגלים עניין בסוגיית הרגולציה והשימוש שנעשה באינטרנט. לאחרונה הכריז נאט"ו על מרחב הסייבר כמרחב לחימה אוטונומי. נאט"ו עשה זאת משיקולים פוליטיים ואסטרטגיים, תוך שהוא מאמץ עמדה שאינה בהכרח משותפת לכלל החוקרים את נושא הסייבר.

מאז שהאינטרנט נפתח לשימושם של גופים מסחריים בשנות התשעים של המאה העשרים, רכשו לעצמם גורמים מהמגזר הפרטי (ממפעילי רשתות ועד ספקי שירות) מעמד בולט בוויכוח על הרגולציה שלו ועל השאלה האם מרחב סייבר חסר גבולות מציע יתרונות לחברות האינטרנט אך גם מציב אותן בהכרח על מסלול התנגשות עם מדינות ריבוניות? מצדו השני של הרצף נמצאים האזרחים הפשוטים (כגון מפעילים, יצרני תוכן, תושבים, מומחים, עיתונאים וכול משתמש שהוא), המבקשים לגבש תפיסה משלהם לגבי מרחב הסייבר כיום, ובכלל זה האם וכיצד יהיה נתון לשליטה ופיקוח בעתיד.

רקע היסטורי

לא ניתן להבין כהלכה את מרחב הסייבר מבלי להכיר היטב את הרקע ההיסטורי שלו. אין זה מפתיע שהיסטוריית הסייבר היא בעלת עשורים ספורים בלבד. הקצב המהיר של השינויים וההתפתחויות בעולם הסייבר הופך את המבט לאחור לא רק לאפשרי אלא גם לחיוני, במיוחד אם רוצים לבסס את הדיון בסייבר על קרקע יציבה.

ההתפשטות הפתאומית והמהירה של האינטרנט הייתה תוצאה של שורת גורמים טכניים ופוליטיים שהתכנסו יחדיו. סביר להניח שאף אחד מהשחקנים המעורבים לא השכיל לצפות את העתיד להתרחש ולא העריך עד כמה מהפכנית תהיה המצאת האינטרנט. בתוך פרק זמן קצר הוא הפך מרשת צבאית ואקדמית בעיקרה, המחברת בין כמה עשרות אתרים ושימושית רק דרך ממשקים של שורות פקודה, למשאב כלל־עולמי הנגיש למיליוני בני אדם, המשתמשים בממשק "הצבַּע ולחץ" של דפדפן הרשת.

הטלקומוניקציה הקולית של שנות השבעים והשמונים של המאה העשרים שיקפה עולם אחר לחלוטין מאשר עולם רשתות הנתונים, המערֵב חילופי נתונים ומסרים של מחשב למחשב. חברות הטלקומוניקציה (טלקום) שפעלו בשוק נהנו ממעמד דומיננטי, מונופוליסטי או כמעט מונופוליסטי, ומתזרים מזומנים שהתלווה לכך. אולם בארצות הברית, שבה קיימת מסורת חקיקה בתחום ההגבלים העסקיים עוד מהמאה ה־19, התרחש תהליך מתמשך של דה־רגולציה ועידוד התחרות, שפלל שבירת מונופולים וחברות. חברת AT&T היא דוגמה בולטת לכך. ההשפעה הישירה של תהליך זה הייתה דחיפה לחדשנות בתחום התשתיות.

הליברליזציה של שוק הטלקומוניקציה אפשרה במידה מסוימת לארצות הברית להרחיב את השפעתה גם לשאר העולם המפותח. מהלך מדיני חשוב נוסף הייתה ההחלטה של רשות התקשורת האמריקאית הפדרלית (FCC) לסווג מחדש "עיבוד נתונים" – קרי, תקשורת דיגיטלית בין מחשב למחשב – כשירות המעניק "ערך מוסף", וזאת בניגוד לשירותי הקול הבסיסיים.[1] התוצאה הייתה יצירת שוק פתוח ולא מפוקח של שירותים דיגיטליים, שנעדרו אפילו את מחסומי הסחר המקובלים.[2] שירותי מידע היו בעבר חלק זעיר מהכנסותיהן של חברות הטלקומוניקציה, דבר שהביא לכך ששוק זה נשאר גם עתה ללא פיקוח. סביר להניח שהדבר נבע, כאמור, מהעובדה ששירותי המידע נחשבו לתחום שההכנסות ממנו היו קטנות בהשוואה להכנסות משירותי הקול. בכול מקרה, מדיניות זו סללה את הדרך לרשת מידע דיגיטלית כלל עולמית.

לצד המדיניות הכללית, היו גם כמה היבטים טכניים שתרמו להתרחבות האינטרנט, ובכלל זה לאופן שבו תקשורת הנתונים מנוהלת ברשת. האינטרנט התבסס על טכנולוגיית מיתוג־מנות (packet-switching), המאפשרת לשני צמתים להחליף ביניהם מידע מבלי ליצור נתיב קבוע או אפילו ידוע מראש ביניהם. הנתונים מחולקים ל"מנות" קטנות המשודרות בנפרד, יתכן בנתיבים שונים ואף בסדר שונה מהמקורי. השלם נבנה מחדש ביעד על ידי תוכנת הרשת. תהליך זה היה שונה לחלוטין מטכנולוגיית "מיתוג המעגלים" של רשתות הטלפוניה, שבה מוגדר מעגל (או נתיב) ייעודי בכול פעם שנוצרת תקשורת בין שני צמתים. ארכיטקטורת מיתוג־מנות אפשרה ניהול מבוזר, משום שאת החלטות הניתוב בנוגע למנות הנתונים ניתן היה לעשות ברמה המקומית, ללא צורך במידע מפורט ברשת. לכך הצטרפה העובדה שפרוטוקולי התקשורת הספציפיים ששימשו באותו זמן (TCP/IP) היו סטנדרטיים וציבוריים – החלטה הנדסית שהתקבלה עשרות שנים קודם לצמיחה המהירה של האינטרנט ואפשרה הוספה של רשתות קיימות. למעשה, עד אז פירוש

1 Milton L. Mueller, *Network and States* (Cambridge: MIT Press, 2010).
2 שם.

המילה "אינטר־נט" היה מילולי: חיבור בין־רשתי של שתי רשתות מחשבים או יותר (רק מאוחר יותר היא קיבלה את ה' היידוע והפכה להיות "האינטרנט").

תרומה טכנולוגית נוספת הייתה בשלתה של תנועת התוכנה החופשית שאפשרה, בין היתר מסיבות כלכליות, את זמינותם של מרכיבים שסייעו להקמת מספר רב של חברות אינטרנט ושרתים. GNU/Linux ושרת הווב Apache הם שתי דוגמאות בולטות לכך. אין להמעיט גם בערך כניסתן של טכנולוגיות ה־xDSL, שהביאו לציבור חיבורי פס רחב יחסית.

מתח המשילות

הוויכוח בנושא הפיקוח על מרחב הסייבר נחלק לשתי עמדות מנוגדות. מצד אחד ניצבת ההשקפה הטוענת שמרחב זה הוא מעין ישות נפרדת לחלוטין מהעולם ה"פיזי", ישות שבה המידע זורם בחופשיות ואין חוק המחייב אותה. העמדה המנוגדת גורסת שכול מדינה אחראית לחלקה הריבוני באינטרנט הגלובלי ורשאית ליישם כל מנגנון משפטי כדי להבטיח את ביטחון הפעילות המקוונת החוצה את מרחבי הרשת שלה. עד היום לא הושגו הסכמה או פשרה לגבי עמדות מנוגדות אלו, והסטטוס קוו נותר על כנו, אם כי שאלת המשילות באינטרנט ממשיכה לעורר ויכוח עז.

על פי ההשקפה שלפיה מרחב הסייבר הוא ישות נפרדת מהעולם הפיזי, מדינות לאום אינן רוצות ואינן יכולות לפקח על כל המתרחש באינטרנט. פירוש הדבר הוא שמרחב הסייבר אינו כפוף לדין, לריבונות או לגבולות "הרגילים". גישה זו זכתה לניסוח מוצלח אצל ג'ון פרי בארלו (Barlow), לפיו: "ממשלות העולם המתועש, אתן הענקיות היגעות [...], באתי ממרחב הסייבר, משכנה החדש של הַבִּינָה [...], מקום שבו אין לכן כל ריבונות".[3] כתמיכה באמירה זו ניתן להוסיף כי התכונות הטכניות של האינטרנט – ביזור (הודות לפרוטוקולים של IP) וטבעו המתנייד בקלות של המידע – הן שמעניקות למערכת את עצמאותה מהעולם הפיזי ומהריבונות של מדינות הלאום. התשתית מאפשרת לידה וצמיחה של ארגוני רשת, המורכבים מחברי קבוצה ומִקשרים בלתי תלויים לחלוטין במיקומים פיזיים, בסמכויות שיפוט או בגבולות. הארגון הפנימי של חברי הקבוצה בתוך אותם מבנים חברתיים – בין אם מדובר בארגוני חברה אזרחית, במועדונים המשקפים אינטרסים מיוחדים או ברשתות חברתיות – תלוי אך ורק בזרימת המידע.

עקרון היסוד של מה שניתן לכנות "ליברטיניות הסייבר" הוא שאין צורך בפיקוח ריבוני ובחוקים במרחב הקיברנטי. אלא שלמרבה הצער, עוצמתם של ארגונים

3 John Perry Barlow, "A Declaration of the Independence of Cyberspace", in *Crypto Anarchy, Cyberstates and Pirate Utopias*, ed. Peter Ludlow (Cambridge: MIT Press, 2001).

מרושתים יכולה לשמש גם להקמת ארגוני טרור ופשיעה, המנצלים את האנונימיות היחסית שהסייבר מאפשר. טבעם העל־לאומי של ארגונים אלה מאפשר לחבריהם לתפקד בצורה מלוכדת, למרות שהם פועלים במיקומים גיאוגרפיים נפרדים ותחת סמכויות שיפוט שונות.

ההשקפה השנייה נוגעת לריבונות המדינה במרחב הסייבר. השקפה זו גורסת כי לא רק שהרכיבים הטכנולוגיים של האינטרנט צריכים להיות כפופים לסמכות המדינה, אלא שגם המידע שנוצר, שנכנס אל המרחב הדיגיטלי הריבוני שלה או שחוצה אותו חייב להיות כפוף לה. הפוטנציאל ליצירה ולקיום של רשתות חברתיות על־לאומיות בקלות, בגמישות ובאופן אנונימי יחסית, נתפס כאיום הן על ריבונות המדינה והן על הביטחון הלאומי שלה.

תפיסה זו הלכה והתבססה מאז תחילת המאה ה־21, במיוחד נוכח העימות המתמשך עם רשתות הטרור המאורגן. אולם הטרור שפגע באירופה ובארצות הברית אינו המניע היחיד הניצב מאחורי העמדה הדוגלת בריבונות המדינה במרחב הסייבר. התנועות החברתיות שהובילו ל"מהפכות הצבעים" ול"אביב הערבי" הן אות לעשוי לקרות אם מידע ימשיך לזרום ללא פיקוח. יתרה מכך, למדינות לאום יש נטייה טבעית לשמר ולהרחיב את גבולות כוחן. הפוטנציאל של מרחב הסייבר כערוץ לתקשורת וללחימה הופך אותו, לפיכך, לשלוחה טבעית של עוצמת המדינה. ואכן, השליטה על תנודות פיננסיות, ואפילו מדיניות מטבע, הן מאפיינים של ריבונות הנמצאת תחת מתקפה.

מתנגדי תפיסת הריבונות רואים בה כלי המשמש משטרים אוטוריטריים כדי לתת תוקף חוקי לפיקוח ולשליטה על אזרחיהם. ואכן, מתנגדים ואופוזיציה פוליטית הפכו פעמים רבות ליעד למעקב פנימי צמוד, והאיום הקיומי של הטרור, כפי שהוא נתפס על ידי המערב, הפך למהות הקיום של המדינה המפקחת. זאת ועוד, מדינות אוטוקרטיות ופחות דמוקרטיות אינן נזקקות אפילו לנימוק זה כדי לקבוע את גבולות המותר והאסור.

המתח בין שתי ההשקפות השפיע על הוויכוח בנוגע ל"משילות באינטרנט" בשנות התשעים של המאה העשרים, ובמיוחד מאז תחילת המאה ה־21. מתח זה הוביל לשני מודלים של משילות: לפי המודל האחד, מרחב הסייבר נתפס כמשטר בין־לאומי נוסף שיש להסדירו באמצעות אמנות וארגונים בין־מדינתיים (איגוד הטלקומוניקציה הבין־לאומי – ITU – הוא דוגמה בולטת לכך). לפי המודל השני, יש לפעול למען יצירת רשת משילות (המונח הנוכחי של האיחוד האירופי לכך הוא "ריבוי בעלי עניין"). רשת משילות, שתוקם על ידי גורמים ממשלתיים ולא ממשלתיים גם יחד, נתפסת על ידי רבים כמודל המתאים ביותר לאינטרנט, והיא למעשה הדרך שמרחב הסייבר פועל לפיה כיום.[4] החזון של מרחב הסייבר כמשאב

4 Mueller, *Network and States*, ch. 3, p. 31.

כלל עולמי הוא אטרקטיבי אך מטעה: הסייבר הינו תחום מלאכותי לחלוטין, ואין בו אף חלק שמתקיים מחוץ לריבונות כלשהי (אפילו כבלים תת־ימיים הם חלק ממערך שלם של רגולציות ואמנות, שמקורו עוד במאה ה־19).[5]

המתח בין שתי ההשקפות מודגש ביתר שאת נוכח העובדה שמודל של משילות רשתית כבר היה קיים כאשר מדינות החלו להבין את פוטנציאל מרחב הסייבר ולבסס מחדש את ריבונותן המסורתית. תאגיד האינטרנט להקצאת שמות ומספרים (ICANN) והניהול המבוזר של מערכת שמות המתחמים (DNS) הם דוגמאות מובהקות לכך. משילות מבוזרת הפכה את האינטרנט להצלחה הגדולה שהוא מהווה, וקשה לטעון לפיכך את ההיפך.

ההתפתחות האחרונה

מדינות לאום החלו להשיג שליטה על מרחב הסייבר מאז תחילת המאה ה־21. התפתחות זו התפשטה גם אל מחוץ למדינות המערב, שבהן האינטרנט ומרחב הסייבר נתפסים כנשלטים על ידי "הגמוניית הסייבר" של ארצות הברית. אף שההתנגדות ל"הגמוניית הסייבר" משמשת ככלי תעמולה בידי סין, הדבר לא מנע מארצות הברית ומבעלות בריתה הקרובות, ובמיוחד מסוכנויות הביטחון שלהן, מלהחזיק בגישה "ניאו קולוניאליסטית" מסוימת ביחס למרחב הסייבר. דוגמאות בולטות לכך הן פיתוח ופריסה של נשק סייבר, כמו תולעת "סטקסנט" והשפעתה; המתקפה של המודיעין הבריטי על חברת הטלקום הבלגית Belgacom; התביעה לתת תוקף כלל עולמי לדין האמריקאי בתחום הסייבר תוך התעלמות מסמכויות שיפוט אחרות; וצו בית המשפט שחייב את חברת "מייקרוסופט" לשחרר נתונים שאוחסנו באחד ממרכזי הנתונים שלה באירלנד.

כאשר בוחנים את הסוגיה מנקודת מבט זו, הפרקטיקות שנוקטות מדינות דמוקרטיות וליברליות אינן שונות בהרבה מאלו של המדינות הפחות דמוקרטיות. יתרה מכך, פרקטיקות אלו אף סותרות לעתים האחת את השנייה. לדוגמה, הניסיונות ליצור "שוק דיגיטלי יחיד" ללא גבולות בתוך האיחוד האירופי הולכים יד ביד עם יצירה ואכיפה של גבולות חיצוניים שנועדו למנוע הצפה אמיתית או מדומה מצד חברות שמחוץ לאיחוד האירופי, למשל לצורך התחמקות מתשלום מס.

אכיפת גבולות

את המדיניות והפעולות שנוקטות מדינות במטרה לבסס ולאכוף גבולות למרחב הסייבר ניתן לסווג באמצעות בחינת שני משתנים: המשתנה הראשון מתייחס לשאלה האם הפעולה היא "גלויה" או "סמויה" (covert/overt). השימוש במונח

5 Alessandro Guarino, "Cyberspace Does Not Exist", *Strange Loops*, January 15, 2015, http://www.studioag.pro/en/2015/01/la-nuvola-non-esiste/.

"סמוי" בהקשר זה הוא חופשי למדי וכולל שילוב של שתי המשמעויות – סמוי וסודי – כאשר סמוי, בניגוד לסודי, פירושו הסתרת המקור. המשתנה השני קשור לשאלה האם לכללי המדיניות יש אופי טכני או לא, ובמילים אחרות, האם הם טכניים או משפטיים/פוליטיים באופיים.

מדיניות של מאמצים לא טכניים גלויים תהיה ניסיון להחזיר את משילות האינטרנט לחיקה של המדינה, ישירות או באמצעות ארגונים בין־ממשלתיים. פעולות גלויות אחרות הן כאלו שנגזרות מטבעו הפיזי של מרחב הסייבר. כל התקני הרשת (שרתים, נתבים, תשתית הכבלים, תחנות לוויין) ממוקמים בטריטוריה ריבונית של מדינת לאום וכפופים לחוקיה (או לדין הבין־לאומי במקרה של כבלים תת־ימיים חוצי אוקיינוס). אמנם, קשה לנטר ולשלוט בזרימת הנתונים, אך ניתן ליצור ולאכוף חוקים ותקנות להיבט הפיזי של "הענן".

פעולה פוליטית גלויה יכולה גם לאפשר פעולה טכנית גלויה, כשזו מגובה בהנמקה משפטית (לפחות כלפי המדינה הנוגעת בדבר). "חומת האש הגדולה" של סין היא דוגמה מצוינת לכך. החלטות מדיניות יצרו ארסנל שלם של אמצעים טכניים שנועדו לבסס מחדש את ריבונותה של סין על חלקה "הלאומי" במרחב הסייבר. מדובר באמצעים הנעים מביקורת וסינון מעמיקים של חבילות נתונים בנתבים ההיקפיים, דרך חסימה והחרמה של אתרי אינטרנט, ועד מניפולציה של ה־DNS בתוך סין – ואלו רק חלק מהדוגמאות. במילים אחרות, קל להשיג שליטה ברמה הפיזית, אולם קשה לעשות זאת ברמה גבוהה יותר, כמו עם פרוטוקול TCP/IP ועם ניתוב. בניגוד לכבל פיזי, טכנולוגיית מיתוג־מנות מקשה על השליטה בנתיב שהיא עוברת (למשל, אילו טריטוריות לאומיות היא חוצה).

הצד הסמוי של סיווג מטריציוני אידיאלי יכלול את הרמה הטכנית, שבה מדינות שונות נמצאות במרוץ למיליטריזציה של הרשתות הגלובליות, וזאת מתוך רצון להשיג את היתרון הווירטואלי שיאפשר להן לגנוב מידע בשיטה הקלאסית של ריגול ולהיות מוכנות ללוחמת סייבר עתידית. היערכות כזאת פירושה גם יכולת להגן על רשתות קריטיות של המדינה מפני חדירות. דוגמאות לאמצעים לא טכניים סמויים הן ניטור תוכן ברשתות חברתיות ואחרות, אותו מבַצעות סוכנויות ביטחון ומודיעין. באופן כללי ניתן לומר כי ממשלות המחליטות על מדיניות סמויה, מאפשרות לסוכנויות הביטחון הפנימיות שלהן שליטה על זרימת המידע. דוגמה רלוונטית אחרת לאמצעים לא טכניים סמויים היא "שכנוע מוסרי" שמפעילות ממשלות על ספקי שירותי אינטרנט (ISP) ושאר מפעילי רשת, וזאת כדי להבטיח את שיתוף הפעולה שלהם לצורך שליטה על זרימת המידע (לדוגמה, באמצעות התקנת ציוד יירוט ממשלתי אצלם).[6]

6 James Bamford, *The Puzzle Palace* (New York: Penguin, 1982), pp. 302-305.

חציית גבולות

ניתן לציין כמה מניעים לרצונן של מדינות להותיר את מרחב הסייבר ללא חסימות והפרעות, או לרצונן להגביל אותו באמצעות הגברת השליטה, הפיקוח והמעקב. באופן טבעי, מדינות עשויות לרצות לחצות גבולות כדי לקדם מסחר ותקשורת, או מנגד, כדי לגנוב סודות ולשבש מערכות. הסביבה החוקית (או היעדרה) היא אחת הדרכים המרכזיות של מדינה לשמר את הסטטוס קוו.

מדינות פועלות כיום במטרה להגדיר התנהגות מקובלת במרחב הסייבר. לדוגמה, בסיום מפגש G–20 שנערך ב־2015, הצהירו נציגים בכירים של המדינות החברות על התחייבות להימנע מריגול כלכלי בסייבר לצורך קידום אינטרסים מסחריים.[7] למרות הכרזות חגיגיות אלו, ריגול בסייבר נותר אמצעי אטרקטיבי לגניבת מידע ולמעקב אחר ידידים ואויבים כאחד. סביר להניח שהתחייבות חברות ה־G–20 תביא לכך שמדינות יקפידו לערפל את פעילויותיהן בתחום הסייבר יותר משיחדלו מהן לחלוטין.

מכיוון שממשלות מבקשות לחזק את קשריהן הכלכליים האחת עם השנייה תוך שימוש בסייבר כאמצעי מסייע, גבולות הסייבר שמדינות כמו סין ורוסיה מעוניינות לחזק, הופכים קשים יותר ויותר להגדרה. מצב זה מותיר את המדינות בעמדה לא פשוטה, לפיה כל אחת מנסה להגן על חלקה באינטרנט, ובמקביל מנסה להרחיב את קשריה המדיניים והכלכליים עם שותפותיה הגלובליות.

טכנולוגיות מסייעות לחציית גבולות

אין הגדרה גלובלית מוסכמת למרחב הסייבר. משרד ההגנה של ארצות הברית מגדיר מרחב סייבר כ"תחום המאופיין בשימוש באמצעים אלקטרוניים ובספקטרום האלקטרומגנטי כדי לאחסן, לשנות ולהחליף נתונים דרך מערכות רשת ותשתיות פיזיות משויכות".[8] כלומר, המינוח האמריקאי מתמקד בארכיטקטורת הרשת ובתהליכים המתרחשים במרחב הדיגיטלי. לעומת זאת, רוסיה מעדיפה להשתמש במונח "מרחב מידע", אותו היא מגדירה כ"ספרת הפעילות הקשורה לתצורה, יצירה, המרה, העברה, שימוש ואחסון של מידע, ואשר יש לה השפעה על תודעה חברתית ופרטנית, על תשתית המידע ועל המידע עצמו".[9] גם סין רואה את מרחב

7 Emilio Iasiello, "G20 – No Commercial Hacking by Anyone", *Dead Drop*, January 14, 2016, http://deaddrop.threatpool.com/g20-no-commercial-hacking-by-anyone/.

8 US Department of Defense, *Joint Terminology for Cyberspace Operations – Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, and the Directors of the Joint Staff Directorates* (November 2010).

9 Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English" (Tallinn: Fifth International Conference on Cyber Conflict, 2013).

המידע כישות הוליסטית. ההגדרה הסינית היא כדלקמן: "הפונקציה המרכזית של מרחב המידע היא רכישה ועיבוד של נתונים על ידי אנשים [...] מקום חדש לתקשר עם אנשים ופעילויות. זהו שילוב של כל רשתות התקשורת, מסדי הנתונים והמידע בעולם, המעצב 'סביבה' עצומת ממדים, מקושרת הדדית, בעלת מאפייני אינטראקציה אתניים וגזעיים מגוונים, במרחב שהוא תלת־ממדי".[10]

למרות ההבדלים ביניהן, כל שלוש ההגדרות מתייחסות להיבטים הרשתיים של תחום הסייבר, שהוא מעשה ידי אדם. סביבה כה מורכבת תכלול בהכרח, בין יתר נקודות התורפה שלה, שגיאות אנוש. אלה שעזרו לעצב את הרשת במהלך השנים התמקדו באתגרים הטכניים של העברת מידע במהירות ובאמינות, ולא צפו כי משתמשי האינטרנט עצמם יעשו שימוש באותה רשת כדי לתקוף האחד את השני.

מתקפות ושימוש לרעה אינם חייבים להיות משוכללים כדי להצליח, אך ככול שהגורמים התוקפים או העוינים מיומנים יותר, כך הם מפגינים יכולת ליצור כלים ייחודיים, לנצל נקודות תורפה ולהסב נזקים, תוך שהם מצליחים להישאר סמויים מן העין. להלן כמה טכניקות באמצעותן מצליחים גורמים כאלה לחצות גבולות סייבר של מדינת לאום:

- **הצפנה**: הגורמים הפועלים מנצלים את ההצפנה לצורך הסוואת הנתונים שקצרו והגנבתם אל מחוץ לארגון (Exfiltration). בחלק מהמקרים, הם מסתירים את המידע בקבצים תמימים למראה (סְטֶגָנוגרפיה). טקטיקות אחרות כוללות דחיסה (הקטנת גודל הקבצים מבלי להסיר מידע); הקבצה (Chunking – פירוק הנתונים לחלקים קטנים כך שיתערבבו טוב יותר בתעבורה הרגילה); ערפול (Obfuscation – הסוואת מאפיינים לקוד הקסדצימלי כדי למנוע את זיהוי הנתונים). הצפנת הנתונים מאפשרת לגורמים הפועלים להקשות על הארגון הנפגע בחשיפת סוג המידע שנגנב, וכך הם מונעים את עצם הפתיחה בחקירה בעקבות גילוי הפריצה ואת שיקום הנזקים, לא כל שכן את המאמצים לגלות מי עומד מאחורי המעשה.
- **רשת TOR (The Onion Routing)**: למרות שישנו ויכוח האם תוכנת TOR היא אנונימית לחלוטין, היא נותרה דרך פופולרית בידי הגורמים הפועלים לבצע את תוכניותיהם. כוחה של רשת TOR נשען על העובדה שתיאורטית לא ניתן לדעת איזה מחשב ביקש את התעבורה, שכן המחשב יכול להיות יוזם הקשר או רק הצומת שפועל כממסר לצומת TOR אחר. לקוח TOR בוחר נתיב אקראי דרך צומתי TOR עד שהוא מגיע ליעד הסופי. בהקשר זה, TOR הוא כלי פופולרי למשתמשים המבקשים לעקוף את מגבלות ובקרות הצנזורה במדינה מסוימת, ובאותה מידה הוא משמש גורמים עוינים. תקרית מ־2014 המחישה כיצד רשת

10 אמיליו אזיילו, "האם נשק סייבר משפיע על כלים צבאיים?", **צבא ואסטרטגיה**, כרך 7, גיליון 1, מארס 2015, עמ' 24–25.

TOR מונפה לפעילות של ניצול רשתות: צומת TOR זדוני שימש לשיגור מתקפות ריגול בסייבר נגד ממשלות אירופיות.

- **העברות נתיקות (Pluggable Transports)**: העברות נתיקות מסוות תעבורת TOR כך שתיראה כמו תעבורה משירותים נפוצים אחרים, דוגמת HTTPS או "סקייפ", או כמו תעבורה רגילה באמצעות שינוי זרם התעבורה ב־TOR בין ה"לקוח" ובין ה"גשר".
- **רשתות וירטואליות פרטיות (VPN) ושרתי "פרוקסי"**: רשתות VPN ושרתי "פרוקסי" מגנים על המשתמש באמצעות הצפנת כל הפעילות אל המחשב ומתוכו. כל עוד המחשב מחובר לרשת וירטואלית פרטית, למפעילי הרשת אין גישה לתעבורה (למשל, לאתרים שהמשתמש ביקר בהם). באופן דומה, שרתי "פרוקסי" משמשים כדי לתווך בין הלקוח ובין השרת, ומונעים את הצורך בתקשורת ישירה בין שני הצדדים. הם מספקים רמה מסוימת של אבטחה משופרת בהגנה על זהות המחשב דרכו מתבצעת הגלישה.

מצוקת דיפלומטיית הסייבר

"הסביבה הדיפלומטית" של מרחב הסייבר ממשיכה להיות דינמית – מצב המזמין פעילות עוינת. המבוי הסתום בתחומים קריטיים של מרחב הסייבר הותיר את הממד המשפטי שלו במצב של חוסר ודאות: מדינות ממשיכות לחצות גבולות קיימים מבלי שיהיו לכך השלכות משפטיות כלשהן ברמה הבין־לאומית. במקביל הן נאבקות להגיע להסכמות על הגדרות וסוגיות מפתח משפטיות, כגון טרמינולוגיה לאבטחה וללוחמת סייבר, בעודן נמנעות מלקבל על עצמן אחריות מדינתית. הדבר דומה לשאלת הריבונות בתחום הסייבר. כך, למשל, סין ממשיכה לקדם את ריבונותה במרחב הסייבר כשלוחה של ריבונותה הטבעית – זכות המוקנית לה מתוקף מגילת האו"ם. ארצות הברית, ובמידה מסוימת גם בעלות בריתה, מאמינות כי האינטרנט, בהיותו פלטפורמה גלובלית של קישוריות הדדית, חייב להישאר פתוח לכול (חשוב לציין שבעוד שזו עמדתה הרשמית של ארצות הברית, קיימות עמדות אחרות בתוך הממשל האמריקאי הנוגעות לאסטרטגיות הסייבר, שלעתים אף סותרות האחת את השנייה).

משילות באינטרנט היא זירה למחלוקת מרכזית נוספת. נכון להיום, אין ארגון יחיד המשפיע על האופן שבו האינטרנט אמור להתרחב, על הטכנולוגיות שישמשו בו או על הכללים שישלטו ברשת הגלובלית. סין ורוסיה מעדיפות ארגון ממשלתי בין־לאומי, דוגמת ITU (שהינו חלק ממערך האו"ם), שיפקח על כלל הפעילות באינטרנט וינהל אותה. הודו ישרה קו עם עמדה זו באפריל 2016. לפחות מבחינה רשמית, ארצות הברית מעדיפה גישה של ריבוי מעורבים, שתכלול לא רק ממשלות

אלא גם את המגזר הפרטי, האקדמיה, החברה האזרחית והקהילה הטכנולוגית.[11] הוויכוח בין שתי העמדות חשוב, והצדדים ממשיכים לנסות ולגייס בעלי ברית לקידום עמדותיהם.

תחום משפטי שלישי שנותר לא מוגדר נוגע לשאלה מהו "נשק מידע". סין ורוסיה הציעו ב־2011 לאסור את השימוש בכול "נשק מידע" וטכנולוגיות הקשורות בו, ועשו זאת בנוסח ההצעה הראשונית לקוד האתי שהובא בפני העצרת הכללית של האו"ם. הגרסה החדשה של הקוד, משנת 2015, השמיטה איסור זה נוכח החשש שהכללתו עלולה להתפרש כרמז לכך ששימוש במידע עשוי לעודד אי־יציבות אזרחית, כפי שאכן קרה במהלך "האביב הערבי".

עמדתה המסורתית של ארצות הברית היא התנגדות להוצאת נשק סייבר התקפי אל מחוץ לחוק. הגורם במחלקת המדינה של ארצות הברית האחראי לנושא הסייבר סבור שאמנות צבאיות או דיפלומטיות קונבנציונליות אינן מתאימות למרחב הסייבר, ובמקום זאת מעדיף פיתוחן של "נורמות".[12] גישה זו מתנגשת עם תוצאותיו של מחקר שערכו מומחים משפטיים בהזמנת "מרכז המצוינות המשותף להגנת סייבר של נאט"ו".[13]

מציאת בסיס משפטי משותף היא משימה קשה להשגה אפילו בקרב מדינות "ידידותיות". כך, למשל, ישנם הבדלים מהותיים בין ארצות הברית ובין האיחוד האירופי בגישות המשפטיות כלפי מושג הפרטיות, דבר שהוביל לביטול הסכם "נמל מבטחים" (Safe Harbor) להעברת נתונים בין שני הצדדים. גם הסכם המסגרת החדש – "מגן פרטיות" (Privacy Shield) – נראה כבנוי על בסיס רעוע.

סביבה פוליטית

סביבות פוליטיות תורמות גם הן להתחמקות של מדינות מקביעת גבולות. ממשלות מסוימות יוצרות סביבה מתירנית המאפשרת לפעילויות מסחריות, פליליות או לכול פעילות עבריינית אחרת לעבור דרך המרחב שלהן. הדבר קורה בין אם ממשלות אלו מונעות במכוון חקיקה פנימית ובין אם הן בוחרות באכיפה סלקטיבית של החוק. סביבות פוליטיות אלו אינן תוצאה ישירה של משטרים או של שיטות ממשל מסוימות, אלא בעיקר של אינטרסים של ממשלות המאפשרות את קיומן של פעילויות אלו.

---

11 US Department of State Fact Sheet, "Internet Governance", August 2015, https://www.state.gov/documents/organization/255010.pdf.

12 Kenneth Corbin, "State Department Argues Against Cyber Arms Treaty", *CIO*, May 26, 2016, http://www.cio.com/article/3075442/government/state-department-argues-against-cyber-arms-treaty.html.

13 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

לשם דוגמה, הסביבה הפוליטית ברוסיה מפגינה סובלנות כלפי פושעי סייבר ופצחנים (האקרים) לאומניים. על פי ארגון "עיתונאים ללא גבולות", רוסיה מנהלת מערך של מעקב ופיקוח הדוקים בשם SORM, כאשר SORM–1 מתמקד ביירוט תקשורת טלפונית, SORM–2 מתמקד בנתונים המועברים דרך האינטרנט, ואילו SORM–3 יודע ליירט כל סוג של תקשורת וכולל אחסון לטווח ארוך. ישנה ברוסיה גם אכיפה קבועה של צנזורה.[14] כאשר מדובר במרחב הסייבר, דומה שפושעי הסייבר הרבים ברוסיה פועלים על פי שני כללים בסיסיים: רוסים לא פורצים לרוסים; אם המודיעין הרוסי מבקש עזרה, הם נענים.

הפצחנים הרוסים זכו לתשומת לב מאז מתקפות DDoS נגד אסטוניה ב־2007 ומעורבותם בעימות בגיאורגיה ב־2008. פצחנים לאומנים רוסים היו מעורבים במהלך תקריות אלו במתקפות סייבר בשם ההגנה על התרבות והלאומנות הרוסיות, כאשר חלק מהמתקפות הגיעו מהמרחב האינטרנטי הרוסי או חצו אותו. לאחרונה התרחשה פעילות דומה באוקראינה, שם מתנהל עימות בין אוקראינים לבדלנים רוסים, והמתקפות המקוונות מתקיימות ברמת תכיפות גבוהה.

שלא כמו רוסיה, הסביבה הפוליטית בארצות הברית אינה תומכת ואינה מגלה סלחנות כלפי פעילויות של גורמים לאומנים העוסקים בפיצוח בשם מה שהם קוראים אינטרסים אמריקאיים. עם זאת, העובדה שפצחן אמריקאי בשם "The Jester" מבצע מתקפות נגד טרוריסטים ושאר פעילויות "אקטיביסטיות", מבלי שייחקר או ייעצר על ידי רשויות החוק, מעלה את האפשרות שיש לו אישור לעשות כן. יותר מכך, הסביבה הפוליטית בארצות הברית היא כזו, שבה הרמות הגבוהות ביותר בממשל מעלימות עין ממעקבים מפוקפקים, שבמסגרתם נאספות כמויות ענק של נתונים לא רק ברחבי העולם, אלא גם בתוך ארצות הברית עצמה, וזאת מבלי ליידע את האזרחים או לקבל את אישורם. לאור זאת ניתן לומר שממשלת ארצות הברית חוצה את גבולותיה שלה ועושה שימוש ביכולות המעקב הטכנולוגיות החזקות שלה כדי ליירט ולאחסן מידע נגד מדינות יריבות, אך גם נגד מדינות ידידותיות, ואף נגד אזרחיה שלה.

סמכות חוקית

למרות שפשעי סייבר על־לאומיים משפיעים על כלל המדינות בעולם, ממשלות רבות עדיין לא הסדירו חקיקה מספקת בנושא זה, באופן שיאפשר חקירה והעמדה לדין על פשעים כאלה. גם במדינות שקיימת בהן חקיקה, עדיין לא הוכח שהיא מצליחה להרתיע מפני פעילות כזו. לדוגמה, בארצות הברית נחקקו כמה מהחוקים

14 "Russia: Control from the Top Down – FSB (The Federal Security Service of the Russian Federation)", *Reporters without Borders*, March 11, 2014, https://12mars.rsf.org/2014-en/2014/03/11/russia-repression-from-the-top-down/.

המחמירים ביותר לגבי פשעי סייבר בעולם, וקיימת יכולת אכיפה בתחום זה, שהולכת וגדלה, ואף על פי כן, ארצות הברית היא עדיין מהמדינות המובילות בפשעי סייבר.

שיתוף הפעולה הבין־לאומי בין רשויות האכיפה הוא במקרה הטוב נקודתי. מציאות זו מחייבת את אנשי החוק שוב ושוב ל"משחקי תופסת" עם גורמי פשיעת הסייבר. אין חקיקה בין־לאומית מוסכמת בנושא פשיעת סייבר, למרות ש"האמנה לפשעי סייבר" של מועצת אירופה (האמנה הבין־לאומית הראשונה שמתייחסת לפשעים באינטרנט) עשתה מאמצים רבים לגייס מדינות לפעולה בתחום זה. מה שקורה לעתים הוא ששיתוף הפעולה בין המדינות נגד פשיעת סייבר הינו מוגבל, או שבעיות של סמכויות שיפוט מעכבות את התקדמות החקירות בתחום זה. המציאות היא שלא כל גופי האכיפה עשו את הצעדים הנדרשים כדי להגיע לרמה מתקדמת בלחימה בפשיעת הסייבר, ובמקרים מסוימים אף קורה שגוף אכיפה אחד מסרב לסייע לגוף אכיפה אחר.

נכון להיום, דומה שרק "האמנה לפשעי סייבר" מציעה מענה בצורת שיתוף פעולה נגד פשעי סייבר חוצי גבולות. זאת, במקום שניתן יהיה להסתמך על הסכמים משפטיים בילטרליים בין מדינות או על הסכמים פרטניים שיחולו על מקרים ספציפיים. הצדדים החתומים על "האמנה לפשעי סייבר" הסכימו לאמץ חוקים המוציאים סוגים מסוימים של פשעי סייבר אל מחוץ לחוק, ולנקוט פעולה משפטית נדרשת כדי להבטיח שיתוף פעולה באכיפתם. נכון למארס 2016, 48 מדינות אשררו את האמנה, ואילו שש מדינות נוספות חתמו עליה, אך עדיין לא אשררו אותה. סין ורוסיה בולטות בהיעדרותן מרשימה זו.

סין כמשל

סין הציגה בשנת 2010 לראשונה את עמדותיה בנושא הריבונות באינטרנט, ועשתה זאת בנייר עמדה שכותרתו "האינטרנט בסין".[15] המסר הסיני היה ברור: סין מעוניינת לבסס קווים ברורים של ריבונות במרחב הסייבר, כשם שהם קיימים ביבשה, בים ובאוויר. בהמשך לכך, בכנס האינטרנט העולמי של 2015 שנערך בעיר וו ג'ן, נפגשו פקידי ממשל ואנשי עסקים סיניים בכירים עם פקידי ממשל מקזחסטן, קירגיסטן, פקיסטן ורוסיה, כדי לדון בסוגיות הקשורות לאינטרנט. בדברי הפתיחה שנשא נשיא סין, שי ג'ינפינג, הוא הדגיש את הצורך של כל הממשלות לכבד את זכויותיהן של המדינות השונות לפתח ריבונות בסייבר עבור אזרחי כל מדינה.[16] מהלכים אלה היו ביטוי לרצונה של סין לשמור על מעמדה של המפלגה

15 Shannon Tiezzi, "China's Sovereign Internet", *Diplomat*, June 24, 2014, thediplomat.com/2014/06/chinas-sovereign-internet/.

16 "China Allows no Compromise on Cyberspace Sovereignty", *China Daily*, December 17, 2015, http://www.chinadaily.com.cn/world/2015wic/2015-12/17/content_22735756.htm.

הקומוניסטית הסינית, להגן על האינטרסים הטריטוריאליים של המדינה ולשמר את יציבותה. בעידן שבו האינטרנט מחבר בין כל מרכיבי החברה, סין רואה בריבונות על הסייבר מרכיב קריטי בריבונותה הלאומית.[17] יתר על כן, סין רואה בריבונות על הסייבר לא רק אמצעי להבטיח טוב יותר את האינטרסים שלה, אלא גם כלי חשוב לעמידה נוכח פעולות שמטרתן להשיג הגמוניה בתחום הסייבר ולערער את ביטחונה הלאומי של הרפובליקה הסינית. כותבים סינים התייחסו בהקשר זה למה שהם כינו ניסיונות אמריקאיים לשלוט על האינטרנט הגלובלי – חשש שקיבל חיזוק בחשיפות של פיטר סנואדן ב־2013 על המעקבים שארצות הברית מבצעת באינטרנט בכול רחבי העולם. "החופש המוחלט" של מרחב הסייבר אותו מהללת ארצות הברית נתפס בסין כמצב המיטיב עם הביטחון הלאומי האמריקאי, בעודו פוגע בביטחון שאר העולם.

כדי לקדם את ריבונותה בתחום הסייבר, סין נשענת על מגילת האו"ם, בה היא מוצאת הצדקה להרחבת עקרון השוויון הריבוני גם למרחב הסייבר. סין משיגה בכך שתי מטרות: היא ממחישה את כוונתה לעשות שימוש בחוק הבין־לאומי כדי לתמוך בעמדתה; היא מממשת את רצונה לעורר סוגיות אלו בפורומים בין־לאומיים ובפני ממשלים שונים. מינוף הזווית המשפטית מעניק לגיטימיות להצעה הסינית, והשימוש בזירת האו"ם ממחיש את מחויבותה של סין לפעילות רב־צדדית. ואכן, בדצמבר 2015 נאבקה סין לכלול את המילה "רב־צדדי" ("multilateral") במסמך האו"ם העוסק בהנחיות לקווי המדיניות לאינטרנט בעתיד, והצליחה בכך. חשיבות התוספת הייתה בהצביעה על כך שממשלות, ולא ארגונים עסקיים או אזרחיים, הן שצריכות להיות האחראיות לניסוח הכללים בסוגיה זו. אמנם, מסמך האו"ם המדובר אינו מחייב את המדינות החברות בארגון, אך הוא מספק את האיזון הדרוש מול ההנחיות שנוסחו והתקבלו בעבר.

סין אינה פועלת לבדה, אלא מקדמת ריבונות בסייבר בפורומים בין־לאומיים שונים, כמו למשל במדינות BRICS (ברזיל, רוסיה, הודו, סין ודרום אפריקה), ב"ארגון שנחאי לשיתוף פעולה" וב"קבוצת מומחי הממשל של האו"ם".

יש לציין, בהקשר זה, שסין פעלה לחיזוק ההגנה על האינטרסים הביטחוניים הלאומיים המרכזיים שלה באמצעות שורה של חוקים והצעות חוק. דוגמאות לכך הם:

- **חוק אבטחת הסייבר:** בנובמבר 2016 אישרה ממשלת סין את חוק אבטחת הסייבר שלה. החוק מתייחס לאבטחת מערכות מידע ואינטרנט מרכזיות ומחזק את כוחה של הממשלה לתעד ולסכל הפצה של מידע שנקבע כ"בלתי חוקי". שני נושאים מרכזיים בולטים בחוק זה: היכולת לנטר ולשלוט במידע; חובת

17 "Why Does Cyber Sovereignty Matter?", *China Daily*, December 16, 2015, http://www.chinadaily.com.cn/business/tech/2015-12/16/content_22728202.htm.

הציות של ארגונים זרים לכללים. מבקרי החוק ציינו כי הוא מהווה ניסיון של ממשלת סין לחזק את שליטתה על החברה האזרחית במדינה, בעודה מטילה תביעות לא סבירות על עסקים זרים.[18]

- **החוק לניהול ארגונים לא ממשלתיים זרים**: כל ארגוני ה־NGO נדרשים לקבל אישור מגוף מפקח מיוחד כדי שיוכלו לפעול בסין. כמו כן, נאסר על ארגונים סיניים לבצע פעילויות בשם ארגון NGO בלתי מורשה או יחד אתו. למרות שהחוק אינו קשור ספציפית לסייבר, סביר להניח שארגונים לא ממשלתיים הרשומים כנדרש ברשויות הסיניות יחויבו לציית לכול כללי המדיניות המקובלים בנושא השימוש בטכנולוגיה, כפי שתקבע הממשלה הסינית בחקיקתה.
- **חוק הביטחון הלאומי 2015**: החוק נועד לספק מסגרת חוקית לסוגיות הביטחון של סין לנוכח איומים מתעוררים. שיקולים ביטחוניים חופפים ממחישים את התפיסה הסינית, לפיה ביטחון לאומי הוא תהליך משולב מיסודו, שתוצאתו היא "מסלול ביטחון לאומי לפי מאפייניה של סין".[19] עובדה משמעותית היא שהחוק אינו מוגבל לסין בגבולותיה הגיאוגרפיים, אלא כולל גם את מרחבי הקטבים, את החלל החיצון ואת מרחב הסייבר.
- **החוק למלחמה בטרור 2015**: החוק, שהתקבל בדצמבר 2015, מאלץ חברות טכנולוגיה לסייע לממשלת סין בפענוח מידע ומעניק לרשויות הסיניות גישה לנתונים מוצפנים. החוק משלב אמצעים מינהליים, משפטיים וצבאיים כדי לתת מענה למאמצי המלחמה בטרור של סין, ומבטא תפיסה המשקפת את רצונה של בייג'ין לשלב את כל היבטי הביטחון תחת מטרייה אחת של חוק הביטחון הלאומי החדש. חוק הטרור הסיני מתכתב עם הנטייה העכשווית של סוכנויות הביטחון האמריקאיות להחליש את מערכות ההצפנה כדי לאפשר גישה ממשלתית אליהן.[20]

ניתן לראות מאמצים אלה של סין כניסיון להשיג גמישות רבה יותר לנוכח השפעות חיצוניות, ולהפחית מהחובות הכלכליות ו/או הדיפלומטיות הפוטנציאליות שארצות הברית מבקשת לכפות (כגון סנקציות בתחום הסייבר, סנקציות כלכליות, כתבי אישום וכדומה). בנוסף לכך, מהלכים אלה מחזקים את העמדה הסינית,

---

18 Bethany Allen-Ebrahimian, "The Chilling Effect of China's New Cybersecurity Regime", *Foreign Policy*, July 10, 2015, http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/.

19 "China Focus: China Defines Overall National Security Outlook in Draft Law", *Xinhuanet*, April 20, 2015, http://news.xinhuanet.com/english/2015-04/20/c_134166428.htm.

20 Joseph Lorenzo Hall, "Issue Brief: A Backdoor to Encryption for Government Surveillance", *CDT*, March 3, 2016, https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/.

הגורסת כי ממשלות זכאיות לנהל בעצמן את ענייני הסייבר הפנימיים שלהן. ואכן, רבים מהחוקים הסיניים שצוינו לעיל זוכים לביקורת על שהם מקדמים את האינטרסים הכלכליים של סין כמדינה ומחזקים את יכולת הבקרה של הממשלה, וזאת למרות התעקשותה של בייג'ין שהכול נעשה בהתאם לכללי מגילת האו"ם.

מסקנות

הוויכוח בין מדינות הלאום בנושא המשילות באינטרנט נותר סוגיה שנויה במחלוקת. כתוצאה מכך מתרחשת כיום תופעה המכונה "בלקניזציה" של מרחב הסייבר. תופעה זו מקבלת תנופה בשל השילוב בין אינטרסים של ביטחון לאומי, איומים ולוחמה כלכלית בעולם המערבי, ובין רצונן של מדינות לשלוט על דעת הקהל והשיח הפוליטי ולנטר אותם. אכיפת גבולות במרחב האינטרנט תוביל בסופו של דבר לאובדן הזדמנויות רבות במונחים של פיתוח כלכלי, זרימה חופשית של מידע וחופש מקוון. אמנם, נכון שהחזון הנאיבי־משהו של מרחב הסייבר, כפי שהתגלם ב"הצהרת העצמאות" של ברלו, לא התגשם, אולם גם כיום חיוני למצוא את האיזון בין ריבונות לגלובליזציה ובין ביטחון לאומי לחופש.

מחובתן של דמוקרטיות ליברליות ושל ארצות הברית – בעלת ההגמוניה לכאורה – להוביל את המאמצים למציאת פתרון מוסכם בסוגיית הסייבר. לא יהיה זה מציאותי למזער את מעורבותן של ממשלות בתהליך זה, בדיוק כפי שאין זה מציאותי להטיל עליהן בלבד את משימת מציאת הפתרונות, דבר שעלול להוביל להתנערותן מאחריות. לאור זאת, הסכם רב־צדדי, שיתבסס על הצלחת הקווים המנחים לרגולציה של משאבים גלובליים – האיסור על פעילות צבאית בחלל, הבטחת חופש התנועה בימים הפתוחים ואיסור תביעות ריבוניות על אנטרקטיקה – יכול להשיג פתרון בר־קיימא. בניית משילות ארוכת טווח ברשת, שתאפשר הן למדינות לאום והן לצדדים שאינם מדינות לפעול יחדיו, נראית כדרך היחידה העשויה להניב תועלת הדדית לממשלות השונות. בדרך זו הן יוכלו ליהנות מיתרונות מרחב הסייבר מבלי לסכן את האינטרסים הביטחוניים שלהן.