האם נשק סייבר משפיע על כלים צבאיים?

אמיליו אייזלו

מתקפות סייבר נתפסות בכתיבה הצבאית והאקדמית, לרוב, כנשק אסטרטגי אסימטרי וככלי שיש לו פוטנציאל ליצירת שוויון במערכה בין מדינות חזקות למדינות חלשות יותר. עם זאת, אין עדויות רבות לכך שמתקפות סייבר הן אופציה צבאית ממשית בעימות בין מדינות. במקומות שבהם התנהלו מבצעים צבאיים של ממש (כמו אפגניסטן, גיאורגיה, עיראק או ישראל ורצועת עזה), יש מעט מאוד עדויות לצבא המבַצע מתקפות סייבר נגד מטרה צבאית או אזרחית. זוהי עובדה מעניינת, לאור ההנחה שחלק מהמדינות שהיו מעורבות בעימות צבאי או במשימות לשמירת השלום באזורים עוינים מחזיקות ברמה מסוימת של יכולת סייבר התקפית. מאמר זה מבקש להציג טיעון נגדי לרעיון שכלי סייבר הם נשק צבאי אינסטרומנטלי בלוחמה של העידן המודרני. המאמר ייטען כי נשק סייבר הוא אופציה אפקטיבית בזמנים של מתיחות בין מדינות יותר מאשר בעימות צבאי, ואמצעי יעיל לאיתות מסרים יותר מאשר ככלי להשגת יתרון צבאי.

מילות מפתח: התקפת סייבר, נשקי סייבר, לוחמת מידע, סין, רוסיה, ארצות הברית.

מבוא

מתקפות סייבר נתפסות בכתיבה הצבאית והאקדמית, לרוב, כנשק אסטרטגי אסימטרי וככלי שיש לו פוטנציאל ליצירת שוויון במערכה בין מדינות חזקות למדינות חלשות יותר. עם זאת, אין עדויות רבות לכך שמתקפות סייבר הן

אמיליו אייזלו (Emilio Iasiello) צבר מעל 12 שנות ניסיון כחוקר מודיעין סייבר אסטרטגי. הוא מייעץ לארגוני מודיעין צבאיים ואזרחיים של ממשלת ארצות הברית, כמו גם לחברות במגזר הפרטי המספקות מודיעין סייבר.

אופציה צבאית ממשית בעימות בין מדינות. במקומות שבהם התנהלו מבצעים צבאיים של ממש (כמו אפגניסטן, גיאורגיה, עיראק או ישראל ורצועת עזה), יש מעט מאוד עדויות לצבא המבַצע מתקפות סייבר נגד מטרה צבאית או אזרחית. זוהי עובדה מעניינת, לאור ההנחה שחלק מהמדינות שהיו מעורבות בעימות צבאי או במשימות לשמירת השלום באזורים עוינים מחזיקות ברמה מסוימת של יכולת סייבר התקפית. דוגמאות מובהקות יותר מראות כי מתקפות סייבר יעילות יותר במסגרת פעילות לא צבאית, וזאת כנשק סודי המאפשר לשתק מערכות ללא סימנים מוקדמים, וככזה שיש ביכולתו להסתיר את הזהות האמיתית של מי שעומד מאחוריו – באמצעות שימוש ב"ארגוני שליח" (proxy) והישענות על יכולת הכחשה סבירה (plausible deniability).

מאמר זה מבקש להציג טיעון נגדי לרעיון שכלי סייבר הם נשק צבאי אינסטרומנטלי בלוחמה של העידן המודרני. במקום זאת אטען במאמר שנשק סייבר הוא אופציה אפקטיבית בזמנים של מתיחות בין מדינות יותר מאשר בעימות צבאי, ואמצעי יעיל לאיתות מסרים יותר מאשר ככלי להשגת יתרון צבאי. במצבים של עימות בין מדינות, סביר יותר להניח שנטרול המטרות החשובות של היריב ייעשה באמצעות נשק קונבנציונלי, המאפשר לכמת ביתר קלות את מידת הנזק בקרב. השאלה היא, לפיכך, האם נשק סייבר הוא כלי צבאי אפקטיבי?

מינוח

אין קונצנזוס בין־לאומי סביב הגדרת המונחים "מתקפת סייבר" (cyber attack) ו"נשק סייבר" (cyber weapon). עם זאת, קיימת הסכמה כי מונחים אלה פירושם שיגור נוזקה (malware) מתוך כוונה למנוע, לשבש, לפגוע, להרוס או לבצע מניפולציה במערכות מידע או במידע השמור בהן. לצורך המאמר הנוכחי אומצו ההגדרות שלהלן:

- **מתקפת סייבר**: "פעולות המתבצעות באמצעות רשתות מחשב ומיועדות למנוע גישה אל מערכת מידע, רשת מידע או נתונים שנמצאים בהן, לפגוע בהן, ולשבש או להרוס אותן".
- **נשק סייבר**: "קוד מחשב שמשַמש, או מיועד לשמש, לאיום או לגרימת נזק פיזי, תפקודי או מנטלי למבנים, מערכות או יצורים חיים".[1] דוגמאות לכך כוללות מתקפות של מניעת שירות מבוזרת (DDoS), או החדרת נוזקה המיועדת להרוס מערכות מידע או את המידע השמור בהן.

סייבר כנשק אסימטרי

הכתיבה הצבאית על לוחמת סייבר – נושא משנה בתוך נושא העל של "לוחמת מידע" – נוטה לראות בתשתיות קריטיות יעדים מרכזיים לפעולה צבאית במהלך

עימות, שכן תשתיות כאלו נתפסות כמאפשרות את היכולת הצבאית של המדינה. המשרד לביטחון המולדת של ארצות הברית מגדיר תשתית קריטית באופן הבא: "הנכסים, המערכות והרשתות, בין אם פיזיים או וירטואליים, שהם כה חיוניים לארצות הברית, עד שלהשבתה או להרס שלהם יהיה אפקט הרסני על הביטחון, ביטחון הכלכלה הלאומית, בריאות ובטיחות הציבור או כל שילוב של אלה".[2]

מתקפות סייבר בסביבת מידע הן זירה חשובה להקרנת כוח, במיוחד נגד מטרות רכות כמו מערכות תקשורת, נמלים, שדות תעופה, אזורי היערכות, אוכלוסייה אזרחית, תשתית קריטית ומרכזים כלכליים. בהקשר זה, נשק סייבר הוא התגלמות אידיאלית של אסטרטגיה אסימטרית: ככל שתשתית המידע של מעצמה נהנית מתחכום טכני רב יותר, כך היא פגיעה יותר למתקפות סייבר.

הכתיבה על לוחמת מידע במדינות השונות

העיקרון הבסיסי של אסטרטגיה אסימטרית הוא להפוך את מה שנתפס כעוצמתו של האויב לנקודת התורפה שלו. קרוב לוודאי שאין עוד תחום הממחיש זאת כמו תחום הסייבר, שבו מורכבות התוכנה והחומרה מגבירה את האפקטיביות הצבאית והחברתית מצד אחד, אך מהווה נקודת תורפה שניתן לנצלה לרעה מצד שני.

תיאורטיקנים אקדמאיים וצבאיים עוסקים במלחמת מידע מזה שנים רבות. האזכור המוקדם ביותר ללוחמת מידע בארצות הברית היה של ד"ר טום רונה (Rona) – בשנות השבעים של המאה העשרים.[3] האימוץ הצבאי הראשון של המונח היה ב־1992, כאשר משרד ההגנה של ארצות הברית פרסם הגדרה רשמית של לוחמת מידע במסמך המדיניות המסווג שלו – TS3600.1.[4] במהלך השנים עדכן הצבא האמריקאי את ההגדרה, אולם המונח "לוחמת מידע" הפך לחלק מהלקסיקון שלו, גם אם לא היו עדיין אסטרטגיות רשמיות שהכתיבו כיצד ליישמו בעת מלחמה.

ארצות הברית לא הייתה היחידה במשימה של פיתוח חשיבה מתקדמת על טבעה של לוחמת המידע ובשאלה כיצד ניתן למנף אותה להשגת השפעה מרבית. תיאורטיקנים צבאיים של סין ורוסיה כתבו גם הם בהרחבה בנושא זה. כתיבתם הראשונית דמתה ברובה לדברים שפורסמו עוד קודם לכן, ואף על פי כן היו בה רעיונות חדשים לגבי האופן שבו לוחמת מידע יכולה לשמש בזמן מלחמה. חרף ניואנסים תרבותיים, שררה הסכמה לגבי הפוטנציאל של לוחמת מידע לשמש כנשק המגשר על הפער בין החזק לחלש ומספק לצד החלש אמצעים לתקוף את החזק, מבלי להסתכן בעימות חזיתי של כוח מול כוח. המונח "אסימטריות" מדגיש היטב מצב זה, כפי שניסחו זאת ברין וגלצר: "[הדבר] מזכיר במקצת את אמנות המלחמה היפנית של הג'יו ג'יטסו, המבוססת על הרעיון שניתן לגייס את כוחו ועוצמתו של היריב ככלי נגדו, במקום לתקוף אותו ישירות עם הכוח הקיים".[5]

שלא כמו נשק גרעיני, המחייב משאבים ניכרים ויכולת ייצור וניהול, מלחמת מידע והכלים הדרושים לה נגישים בקלות להמונים.

הכתיבה הסינית על לוחמת מידע

הכתיבה המוקדמת ביותר בנושא לוחמת מידע בסין הייתה, ככל הנראה, בספר "לוחמת מידע", שיצא לאור ב־1985 ופורסם מאוחר יותר כמאמר ב־*Liberation Army Daily*.[6] עם זאת, רק במבצע "סופה במדבר" בעיראק ב־1991 הזדמן לתיאורטיקנים סיניים לראות כיצד צבא עושה שימוש בטכנולוגיה מתקדמת כדי להביס את האויב. ב־1995 כתב רמטכ"ל צבא סין, וואנג פּוּ פֶנג, את "האתגר של לוחמת המידע", שבו כָּלל אזכורים רבים ללוחמת המידע של ארצות הברית במבצע נגד עיראק.[7] כותב סיני אחר ראה מערכה זו של ארצות הברית בעיראק כ"טרנספורמציה גדולה", שבה המידע שינה, יחד עם הפיקוד והשליטה, את פני שדה הקרב.[8] מאז ראו חוקרים סיניים ברעיון של "שליטה במידע" את המפתח להשגת ניצחון במלחמות העתיד.

שני מקורות סיניים העוסקים בדוקטרינות צבאיות – "מדע האסטרטגיה" ו"מדע המערכה הצבאית" – מכירים בלוחמת המידע ככלי צבאי חשוב להתגברות על יתרונות של יריב חזק יותר בתחומי הטכנולוגיה והמידע. אסטרטגים צבאיים רבי השפעה מבתי ספר ואקדמיות צבאיים מובילים בסין הציעו לצבא הסיני ליישם מתקפות סייבר או מתקפות של נשק מדויק נגד מטרות תשתית קריטיות, כמו נמלים ושדות תעופה. ואמנם, רבים מהמקורות שנוטים לגישה סמכותנית בחשיבה הצבאית בסין תומכים בסוג זה של פעולה. מחבר המחקר "מדע המערכה הצבאית" טוען כי לוחמת מידע אמורה לשמש:

> ... בזמן ובאזור שהם קריטיים לפעולת המערכה הכוללת, כדי לחסום את היכולת של האויב להשיג, לשלוט ולעשות שימוש במידע, במטרה להשפיע על היכולות של האויב לתצפת, לקבל החלטות או לפקד ולשלוט בחייליו, וכן להפחית ואף להרוס אותן. כל זאת, במקביל לשמירת יכולת הפיקוד והשליטה שלנו, כדי להחזיק בעליונות בתחום המידע ולהשיג עליונות מערכתית ואסטרטגית, וכך ליצור תנאים לניצחון מוחלט בקרב.

תיאוריית "הלוחמה האלקטרונית המשולבת ברשת" (Integrated Network Electronic Warfare – INEW) של סין כוללת מתקפה על רשת מחשבים בעתות מלחמה או שלום, וכן לוחמה אלקטרונית המתנהלת תחת סמכות אחת. המשימה היא לשבש את היכולת של היריב לעבד מידע ולהשתמש בו. האסטרטגיה הסינית מאופיינת ביישום משולב של כלים אינטרנטיים ונשק ללוחמה אלקטרונית נגד מערכות מידע של היריב, וזאת כבר בשלבים הראשונים של העימות.[9] על פי אותה אסטרטגיה, עוצמתן של מתקפות כאלו טמונה ביכולתן להפתיע את האויב.

בטקסט מעורר מחלוקת שחיברו שני קולונלים (לשעבר) בצבא סין, הם שמו את הדגש על הפוטנציאל שיש למתקפות סייבר לפגוע במוסדות פיננסיים של מעצמות זרות,[10] במיוחד כאופציה של מכה ראשונה. על פי ג'יימס מָלְבנון (Mulvenon), מומחה ידוע ללוחמת מידע סינית, "הכתיבה הצבאית הסינית נוטה ברובה להחזיק בדעה כי לוחמת מידע היא כלי לא קונבנציונלי, ולא מכפיל כוח בשדה הקרב [...] שיאפשר לסין להילחם ולזכות במלחמת מידע ללא צורך בפעולה צבאית".[11]

מלחמת מידע היא זירת קרב רחבה, ומרחב הסייבר הוא רק חלק אחד בעולם המידע הגדול יותר. מרחב המידע מתייחס ל"ספֵרת הפעילות הקשורה לעיצוב, יצירה, המרה, העברה, שימוש או אחסון של מידע, אשר יש לה השפעה על התודעה של היחיד והחברה, על תשתית המידע ועל המידע עצמו".[12] על פי השקפתה של סין, התפקיד העיקרי של מרחב המידע הוא "לאפשר לאנשים להשיג ולעבד נתונים [...], מישור חדש לתקשר עם אנשים ועם פעילויות. זהו המרחב המשלב בין כל רשתות התקשורת, מסדי הנתונים והמידע בעולם, היוצר סביבת פעולה".[13] מכאן עולה שסין רואה במרחב המידע טווח איום רחב יותר, המשתרע מעֵבר לעולם הדיגיטלי המוגבל לאינטרנט.

הכתיבה הרוסית על לוחמת מידע

בדומה לסין, גם רוסיה מתייחסת ל"מרחב המידע" כאל מונח הוליסטי. ב־2010 עדכנה ממשלת רוסיה את הדוקטרינה הצבאית שלה, לאחר שהמונח "לוחמת סייבר" בלט בהיעדרו ממנה (בדומה לסינים, גם הרוסים עושים שימוש במונח "מידע" ומעדיפים אותו על פני המונח הפופולרי יותר "סייבר"). עם זאת, היו בדוקטרינה הרוסית מספר אזכורים ל"לוחמת מידע", שעל פי הגדרתם כוללים מתקפות יזומות על מערכות מידע (כלומר, מחשבים) ו/או על המידע השמור בהן. חשוב מכך, הדוקטרינה הרוסית הכירה בכך שמרחב המידע הוא תחום קריטי המחייב הגנה צבאית מפני איומים חיצוניים. עובדה זו מחזקת את הנאמר ב"דוקטרינת ביטחון המידע 2000" של רוסיה, כי הגנה מפני מידע חיצוני מזיק וקידום ערכים פטריוטיים הם יעדים של הביטחון הלאומי.[14] יעדים נוספים מופיעים ב"דוקטרינה הצבאית 2010" של רוסיה וכוללים[15]: "[...] פיתוח מטרות ומשאבים ללוחמת מידע [...] יצירת מודלים חדשים של כלי נשק מדויקים ופיתוח תמיכה מבוססת מידע עבורם [...] יישום מקדים של אמצעים ללוחמת מידע, במטרה להשיג יעדים מדיניים מבלי להשתמש בכוחות צבאיים".

תיאוריית לוחמת המידע של רוסיה מעוגנת ברעיון לפיו היא חייבת "להגיב במלחמה למלחמת המידע שנפתחה נגדה",[16] ומכסה טווח רחב של פעולות, בין היתר מדיניות, כלכליות, תרבותיות וצבאיות. כותבים רוסיים רואים בלוחמת מידע מלחמה המשפיעה על תודעת ההמון, בהיותה חלק מהיריבויות בין המערכות

הלאומיות האזרחיות השונות שמדינות אימצו. אלו הופכות לרלוונטיות כאשר אמצעים מיוחדים מאפשרים להפוך מקורות מידע ל"נשק מידע".[17] גם רוסיה מגדירה "מרחב מידע" כ"מרחב הפעילות הקשורה לגיבוש, יצירה, המרה, העברה, שימוש או אחסון של מידע, אשר יש לה השפעה על התודעה של היחיד והחברה, על תשתית המידע ועל המידע עצמו".[18] לאור זאת, מה שמדאיג את רוסיה במרחב המידע הן ההשפעות הטכניות (כגון הרס פיזי של מערכת מידע) והפסיכולוגיות (דוגמת השפעה ומניפולציה על אוכלוסייה) על המרחב.

הפרשנות הרחבה של מרחב המידע מביאה את רוסיה לראות ב"נשק המידע" (information weapons) מקור לדאגה. על פי הגדרתה, נשק מידע יכול לשמש בתחומים שמעֵבר לסייבר, לרבות בתחום ההכרה האנושית,[19] ולכלול אזורים גיאוגרפיים שבהם מתגוררים דוברי רוסית או אנשים ממוצא רוסי.[20] אין ספק שרוסיה רואה בהצלחות של "מהפכות הצבע" במרכז ובמזרח אירופה ושל "האביב הערבי" דוגמאות לאובדן השליטה החברתית והשליטה במידע.

הכתיבה האמריקאית על לוחמת מידע

לשיטתה של ארצות הברית, מרחב הסייבר כולל את הרשתות והמערכות שמרכיבות את הארכיטקטורה שלו, אך לא את סביבת המידע כולה כפי שגורסות ההגדרות של סין ורוסיה. מחקרים אסטרטגיים ומבצעיים רבים נכתבו בארצות הברית, שבהם הכותבים הביעו דעתם כיצד על הצבא האמריקאי לפעול ב"מבצעי מידע" (Information Operations) בתחום הסייבר, שבהם פעולות סייבר (או "לוחמת סייבר") הן רק אופציה אחת מתוך כמה אופציות. המסמך "האסטרטגיה לפעולה במרחב הסייבר" שפרסם משרד ההגנה של ארצות הברית ב־2011, וכן הפרסום בנושא "מבצעי מידע" (JP 3–13) מטעם המטות המשולבים של צבא ארצות הברית במהדורת 2012, מציגים את החשיבה האמריקאית העדכנית בנושא מרחב הסייבר כזירת קרב. הקמת מטה הסייבר האמריקאי (CYBERCOM) עולה בקנה אחד עם שאיפתה של ארצות הברית לאפשר לה יד חופשית לפעול בתחום הסייבר, במקביל למניעת יכולות דומות מיריבותיה. על פי מסמך האסטרטגיה של משרד ההגנה האמריקאי, מטה CYBERCOM משקף את היעדים הבאים: "[...] להבטיח פיתוח יכולות משולבות באמצעות עבודה צמודה עם מפקדות, שירותים וסוכנויות לענייני לוחמה ועם קהילת הרכש, במטרה לפתח וליישם במהירות יכולות חדשניות במקומות שהן דרושות במיוחד".[21]

המסמך של המטות המשולבים (JP 3–13) מספק מידע לגבי פריסת יכולות הסייבר האמריקאיות ומציג דוקטרינה והנחיות של המטות המשולבים לפעילויות של צבא ארצות הברית במבצעים משותפים. על פי המסמך: "[...] מִבצעי מידע (לרבות פעולות ברשתות מחשב) מיועדים להשפיע על, לשבש את, או להשתלט

על, יכולת קבלת ההחלטות של יריבים קיימים ופוטנציאליים, במקביל להגנה על היכולת שלנו".[22]

שורש ההבדל בין הכתיבה של סין ורוסיה לזו של ארצות הברית מצוי בפרשנות ההוליסטית של מרחב האיום אצל הראשונות לעומת פרשנות צרה יותר שלו אצל האחרונה. רוסיה וסין מעדיפות לשלב את ההיבט האנושי עם ההיבט הטכנולוגי, בעוד שארצות הברית מתמקדת בהיבט הטכנולוגי בלבד. ארצות הברית רואה את המערכה הגדולה של מִבצעי מידע כמורכבת מכמה יכולות צבאיות הנפרדות זו מזו, אם כי כאלו שעשויות להיות קשורות זו לזו. לעומתה, רוסיה וסין מציגות תפיסה לפיה קיימים קשרים הדדיים הדוקים יותר, שבהם אין הבחנה ברורה בין הפעילויות שבוצעו והתוצאות שהושגו. לאור זאת, מתקפת סייבר יכולה להיות, על פי ההשקפה האמריקאית, החדרת נוזקה לתשתית קריטית, ועל פי ההשקפה הרוסית/סינית – מידע עוין המשוגר על ידי גורמים יריבים ומכָוון נגד הממשלה או הציבור שעליו היא שולטת.

אירועי מתקפת סייבר

כמה ממתקפות הסייבר שזכו לפרסום חושפות את ההתפתחות של נשק הסייבר מכוח משבש לכוח הרסני. אין בכך כדי לומר שכל מתקפות הסייבר בעתיד יכללו הרס של מערכות מידע, אלא שיש תקדימים לכך שהרס נתפס כבר בעבר כאופציה מועדפת במקרים מסוימים שבהם הצדדים היריבים שרויים במבוי סתום דיפלומטי. במקרים שיפורטו להלן היה חשד לקיומה של יד מכוונת מדינתית, או לחסות של מדינה, אך הדבר לא הוכח מעולם. דבר זה מלמד שאם ממשלות עומדות מאחורי ניהול מתקפות סייבר, הן מעדיפות להשתמש בהן כנשק הפתעה בזמנים של מתיחות דיפלומטית, תוך שמירה על יכולת הכחשה סבירה ועל מינימום של עימות חזיתי, אם בכלל.

וירוס "וַויפֶּר", קוריאה הדרומית, 2013

במארס 2013 מחקה הנוזקה "וַויפר" (wiper) נתונים ממערכות מחשב של שלושה בנקים בקוריאה הדרומית ושל חברות הביטוח שלהם, וכן של שלושה גופי שידור. מרבית המתקפות התרחשו ב־20 במארס, אך העדויות מלמדות שבחלק מהמקרים המערכות נדבקו עוד קודם לכן בווירוסים, ואלה כָוונו להפעלה בתאריך המיועד.[23] הווירוס "וויפר" מחק את רשומת האתחול הראשית במחשבים השולטים ברשתות התקשורת של גופים אלה, וכן השבית את תוכנת האנטי־וירוס של חברה דרום קוריאנית ידועה.[24] לפי ההערכות, המתקפה פגעה ב־48,000 מחשבים.[25]

היה זה האירוע הרביעי בסדרה של מתקפות הקשורות לווירוס "וויפר" שזכו לפרסום. המתקפה הראשונה התרחשה באפריל 2012 נגד מתקן אירני באי חארג'.

השנייה הייתה בחברה הסעודית "עראמקו" והשלישית הייתה בחברה הקטרית "ראסגָז". מתקפות אלו היו איתות לכך שגורמים לא מדינתיים מוכנים לעבור לפעולות הרסניות יותר בעתות של מתחים פוליטיים. כמו באירוע ב"עראמקו", גם במקרה של קוריאה הדרומית נטל את האחריות ארגון לא מוכר בשם WHOIS,[26] למרות שהיו מי שהטילו ספק באמינות הודעתו עקב היעדר מידע על עברו או עדות ליכולתו לבצע מתקפה ברמה כזו.

גורמים רשמיים בקוריאה הדרומית מאמינים שיחידות המודיעין הצבאי של קוריאה הצפונית הן שאחראיות למתקפה, תוך שהן פועלות מכתובות IP סיניות.[27] על רקע המתיחות המתמשכת בין קוריאה הצפונית לקוריאה הדרומית, אירע לא פעם, לפחות מאז 2009, שהרטוריקה המדינית והדיפלומטית בין הצדדים גלשה לעולם הסייבר, כאשר רשתות "סוכני תוכנה" (botnet) כיוונו מתקפות למניעת שירות מבוזרת (DDoS) נגד אתרי אינטרנט של ארצות הברית וקוריאה הדרומית.[28] קוריאה הצפונית אף הגבירה את איומיה על קוריאה הדרומית וארצות הברית במהלך התרגיל הצבאי השנתי המשותף של השתיים, Key Resolve, שנערך ב־11 עד 21 במארס 2013 (זמן קצר לאחר שבפברואר 2013 ערכה קוריאה הצפונית ניסוי במתקן הגרעין שלה).[29] אם קוריאה הצפונית אכן עומדת מאחורי מתקפות אלו, הרי שיש בכך סטייה מהשיטה שנהגה בה עד אז – בדרך כלל פעילות נמרצת למניעת שירות, אך למעשה כזאת שלא גרמה נזק של ממש. חשוב מכך, התקרית של מרץ 2013 אותתה לממשלת קוריאה הדרומית שקוריאה הצפונית מסוגלת לבצע מתקפות סייבר הרסניות כאשר היא מעריכה שהייתה הפרה של ה"נורמות" שהתבססו בין שתי הקוריאות.

וירוס "וייפר", "עראמקו", 2012

באוגוסט 2012 גרם וירוס שכונה "שאמוּן" למחיקת נתונים ב־75 אחוזים מכלל מחשביה של חברת "ערמאקו" – חברת הנפט הלאומית של ערב הסעודית ומי שנחשבת לחברת הנפט בעלת הערך הגבוה בעולם.[30] הנוזקה נועדה להשיג שתי מטרות: להחליף את הנתונים בכוננים הקשיחים בתמונה של דגל אמריקאי העולה באש ולהעביר רשימה של כתובות נגועות למחשב שנמצא בתוך הרשת של החברה; למחוק את הזיכרון במחשבים הנגועים.[31] הווירוס הרס את הכוננים הקשיחים של 30,000 מחשבים.[32]

חשיבות האירוע נעוצה בכך שמדובר בנוזקה שהוטמעה מתוך כוונה להרוס כוננים רבים ככל האפשר במחשבים של חברה הקשורה לתשתית קריטית. התחכום של הנוזקה נתון לוויכוח. שר ההגנה של ארצות הברית דאז, ליאון פָּנֶטָה, התייחס לווירוס "שאמון" כאל כלי מתוחכם מאוד,[33] ולעומתו סברו חוקרי אבטחה ממעבדת קָסְפֶּרסקי ששגיאות הקידוד בקוד היו אינדיקציה לעבודה חובבנית ושלווירוס

היה פוטנציאל להיות הרסני אפילו יותר.[34] הווירוס "שאמון" הופעל נגד חברת "עראמקו" יום לפני אחד המועדים הקדושים ביותר בשנה המוסלמית.[35] ניתן לשער שהתוקפים ביקשו להגביר את הצלחתם המבצעית כשהעריכו, ובצדק, שבמועד זה ניטור המחשבים יהיה מצומצם יותר, דבר שייתן זמן נוסף לווירוס להתפשט. ואכן, המתקפה השפיעה על ייצור הנפט ועל ההתנהלות העסקית של החברה, עקב איבוד חלק מנתוני הקידוח והתפוקה.[36] על פי אחד המקורות, נדרשו עשרה ימים להחליף את הכוננים הנגועים.[37]

ארגון לא מוכר בשם "חרב הצדק" קיבל על עצמו את האחריות למתקפה על מחשבי "עראמקו", בטענה שזו תגובה למדיניות הסעודית במזרח התיכון.[38] למרות זאת, רבים, וביניהם גורמים אנונימיים בממשל האמריקאי, חשדו שמדובר במעורבות איראנית.[39] אם איראן אכן עמדה מאחורי המתקפה, פירוש הדבר שהיא מעדיפה לתקוף את ערב הסעודית בחשאי באמצעות "שליח", כדי לשמור על יכולת הכחשה סבירה, במיוחד לאור העובדה שהמתקפה כוונה ישירות נגד יצרנית נפט גלובלית מרכזית ונגד תשתית קריטית.

אין כיום קונצנזוס בין־לאומי סביב השאלה מה מהווה "קו אדום" בתחום הסייבר, ואף על פי כן ניתן להניח שפעולת הרס מכוונת נגד ארגון בעל ממדים גלובליים תיחשב לצעד תוקפני (act of force) על פי דיני המלחמה במשפט ההומניטרי הבין־לאומי, המסדירים פעולות איבה חמושות בין מדינות לאום. בהקשר זה, ניתן לפרש את הפגיעה המכוונת בחברת "עראמקו" – סמל לשלטון הסעודי – כאיתות איראני לערב הסעודית על חוסר שביעות רצונה של טהראן מכך ש"עראמקו" נהנית מהסנקציות שהטיל האו"ם על איראן, וכן ממה שנראה כשיתוף פעולה סעודי־אמריקאי נגד שאיפותיה הגרעיניות של איראן.

מתקפת "סטוקסנֶט" על הצנטריפוגות האיראניות, 2010

ההערכה היא שווירוס "סטוקסנט" (Stuxnet) קשור קשר הדוק לשלוש נוזקות דומות, ואולי אף מתוחכמות ממנו, המוכרות בשמות Duqu, Flame ו־Gauss. שלוש נוזקות אלו קשורות בעיקר לריגול סייבר, ולפיכך המאמר הנוכחי אינו עוסק בהן.

ב־2010 הודתה איראן כי נשק סייבר, שחוקר בחברת "מיקרוסופט" הדביק לו את הכינוי "סטוקסנט", גרם נזק לצנטריפוגות הגז במתקן שלה להעשרת אורניום. "סטוקסנט" תואר כיישום מורכב ו"מתוחכם במיוחד", שכל תכליתו הייתה לחבל בצנטריפוגות להעשרת אורניום של איראן שנשלטו על ידי "משנה מהירות" (high frequency converter drivers) במתקן להעשרת האורניום בנָתַנְז.[40] כאלף צנטריפוגות נפגעו מהנוזקה, שגרמה להן לצאת מכלל שליטה, ובסופו של דבר היה צורך להחליפן.[41] למרות ש"סטוקסנט" התגלה ב־2010, ההערכה היא שהווירוס חדר לרשת כבר ב־2009,[42] דבר המלמד על יכולת גישה חשאית למטרה.

תקרית "סטוקסנט" הייתה בעלת משמעות רבה, משום שלראשונה נוצר ויושם נשק סייבר במטרה לפגוע, לשבש ולהרוס מערכת מידע מסוימת. חשוב מכך, התחכום של הנוזקה, כמו גם חדירתה החשאית לרשת של מערכת בקרה תעשייתית – למרות שזו הותקנה עם הפרדה פיזית (air gap) מהאינטרנט ופעלה בסביבה מאובטחת – הצביעו באופן ישיר על מעורבות וחסות של מדינה. אף ארגון לא קיבל על עצמו אחריות לאירוע.

איראן הבהירה בכמה הזדמנויות שבכוונתה ליישם את זכותה הריבונית לפתח את תוכנית הגרעין שלה למטרות שלום.[43] דברים אלה עוררו אי־נחת רבה בארצות הברית, כמו גם במדינות מערביות ומזרח־תיכוניות אחרות, וכן ברוסיה ובסין הידידותיות לאיראן.[44] אמנם, אף ממשלה לא קשרה עצמה באופן רשמי ל"סטוקסנט", אך הסברה המקובלת היא שמדובר בפרי שיתוף פעולה בין ארצות הברית לישראל.[45] השימוש המוצלח ב"סטוקסנט" מנע את הצורך בתקיפה צבאית קונבנציונלית על מתקני העשרת האורניום של איראן – מהלך שעלול היה לגרום לפעולת תגמול איראנית מסלימה. אם ארצות הברית אכן עומדת מאחורי "סטוקסנט", ניתן לפרש את הדבר כאיתות לאיראן כי וושינגטון נותרה מחויבת לעמדתה שלא להתיר לאיראן להעשיר אורניום למטרות צבאיות, וכן כהוכחה ליכולתה של ארצות הברית לחדור למתקן רגיש ומאובטח היטב שיש בו נשק להשמדה המונית.[46]

מתקפות מניעת שירות מבוזרת (DDoS), גיאורגיה, 2008

באוגוסט 2008 פלש כוח רוסי לגיאורגיה בעקבות החלטת ממשלתה לפתוח במתקפת פתע נגד כוחות הבדלנים בדרום אוֹסֶטיה.[47] קודם לפלישה הרוסית שוגרו מתקפות סייבר רוסיות נגד אתרי אינטרנט של ממשלת גיאורגיה.[48] מתקפות דיגיטליות אלו, שנמשכו לאורך רובו של חודש אוגוסט, כללו בעיקר השחתה של אתרי אינטרנט (בראש ובראשונה אתרי אינטרנט ממשלתיים) ומתקפות מניעת שירות שכוונו לאתרי תקשורת, מוסדות פיננסיים, אתר של קהילת האקרים בגיאורגיה ואתרים של ממשלת גיאורגיה.[49]

מתקפות סייבר אלו בלטו מסיבה מרכזית אחת: הן התרחשו במקביל לפלישה הצבאית של רוסיה לגיאורגיה. מתקפות הסייבר של 2008 על גיאורגיה היו דומות במובנים רבים למתקפות סייבר שהיו עליה בשנת 2007, מתקפות שכללו השחתת אתרים ומניעת שירות ביעדים של המגזר הפרטי והציבורי במדינה. הייחודיות של מתקפות הסייבר על גיאורגיה הייתה בתיאום ובעוצמה שלהן, וזאת בניגוד למתקפות על אסטוניה, בהן התיאום היה מדורג.[50] אם אותם גורמים עומדים מאחורי אותן מתקפות, הרי שהם שינו את מתודולוגיית המתקפה שלהם כדי להשיג יעילות מרבית.

כמו באסטוניה, גם המתקפות בגיאורגיה יוחסו להאקרים לאומניים רוסיים, וממשלת רוסיה נחשדה כמי שממממנת אותם.[51] אם אכן מוסקבה עמדה גם הפעם מאחורי המתקפות, ניתן לראות בכך ביטוי להפקת לקחים שעשתה בכל הנוגע לפגיעה מכוונת במדינה זרה באמצעות נשק הסייבר. המטרה המרכזית של מתקפת הסייבר באסטוניה הייתה התשתית, ואילו בגיאורגיה היו אלה ארגוני תקשורת וחדשות שהפכו לקורבנות הראשיים שלה. באמצעות המתקפה על גופים אלה, ביקשו התוקפים לשלוט במרחב המידע של גיאורגיה ולמנוע שידור של גילויי תמיכה בהתנגדות לרוסיה. היה זה ביטוי לתפיסה הרוסית של לוחמת מידע, המוצגת גם על ידי תיאורטיקנים רוסיים מובילים בתחום לוחמת המידע, דוגמת איגור פנארין (Panarin).[52]

המאמצים של אלה שקיוו לשלוט במידע בגיאורגיה כשלו בסופו של דבר, ורבים סבורים שגיאורגיה ניצחה במלחמת המידע הזאת.[53] אף על פי כן, התקרית ממחישה כי אפילו במהלך עימות חזיתי בין כוחות, רוסיה מעדיפה לשמור על יכולת הכחשה סבירה בנוגע למעורבותה במתקפות סייבר. לכאורה, ניתן היה להניח שברגע שרוסיה יזמה מתקפה פיזית על גיאורגיה היא לא תראה עוד צורך להסוות את מבצעי הסייבר שלה, במיוחד אם הם לא נועדו להרוס מערכות מידע או נתונים, ועל אחת כמה וכמה כשמדובר במדינה בעלת יכולות סייבר ברמה דומה לזו של ארצות הברית.[54] למעשה, נראה שמתקפות מניעת השירות על גיאורגיה נועדו לאותת לשכנותיה של רוסיה ולמדינות ברית המועצות לשעבר כי עליהן לצַפות לפגיעה דומה בהן, אם ממשלותיהן ייכנסו למצבי מתיחות דיפלומטית עם הפדרציה הרוסית.

עימות צבאי בפועל

לא כל מקרי העימות החזיתי של צבא מול צבא כללו מתקפות סייבר, בין אם כמרכיב מרכזי ובין אם כמרכיב משני. הדבר ראוי לציון לאור העובדה שכמה מהמדינות המעורבות בעימותים כאלה מחזיקות ביכולות הדרושות ללוחמת סייבר, וידוע שהדוקטרינות הרשמיות שלהן כוללות התייחסות לשאלה כיצד מתקפות סייבר עשויות וצריכות להתבצע בתרחישי עימות. ניתן אמנם לייחס את אי־הפעלתן של מתקפות סייבר אסטרטגיות להיעדר מטרות אסטרטגיות למתקפות כאלו, אולם העדויות מלמדות שההימנעות ממתקפות סייבר נבעה בעיקר מהקושי להשיג בדרך זו יתרון אסטרטגי. מצב זה גורם להטלת ספק ביעילותן של מתקפות סייבר כנשק בעל יכולת להשיג תוצאות הדומות לאלו שמשיג נשק קונבנציונלי.

משבר ישראל־חמאס, 2014

ביולי 2014 שיגרה ישראל טיל שפגע בתחנת החשמל היחידה של עזה, ובכך עצרה את אספקת החשמל לאזור. על פי דיווחי העיתונות, מהלך זה היה צפוי להחמיר בעיות של מים וביוב שהיו קיימות עוד קודם לכן.[55] קשה להניח שהשימוש שעשתה ישראל בנשק קונבנציונלי במקרה זה נבע מחוסר היכולת שלה לפגוע באותו מתקן באמצעי סייבר; הדבר סותר את המוניטין שלה כמעצמת סייבר מובילה ואת היותה חשודה במעורבות בכמה מאירועי סייבר מפורסמים, כמו מתקפת הסייבר של 2012 על תחנת כוח איראנית ומתקנים איראניים נוספים,[56] מתקפת ה"סטוקסנט" של 2010 נגד הצנטריפוגות במתקני העשרת האורניום של איראן,[57] או מתקפות הסייבר של 2007 נגד מערכות ההגנה האווירית של סוריה.[58] ניתן להניח שכאשר מדובר במטרה אסטרטגית, כמו השבתת יעד אסטרטגי מרכזי, השימוש בנשק קונבנציונלי הופך לאופציה המועדפת על ישראל, וזאת בשל היותה דרך פעולה אמינה יותר מאחרות להשגת היעדים המידיים.

משבר רוסיה־אוקראינה, 2014

במהלך המשבר בין רוסיה לאוקראינה ב־2014 דיווחה חברת הטלקומוניקציה האוקראינית Ukrtelecom כי חמושים פשטו ב־28 בפברואר אותה שנה על המתקנים שלה בחצי האי קרים, חיבלו בכבלי הסיבים האופטיים והשביתו את פעולת מערכות האינטרנט והטלפון המקומיות.[59] לאור מומחיותה של רוסיה בפעולות סייבר,[60] כמו גם העובדה שחלק גדול מהטלקומוניקציה האוקראינית נבנתה כאשר אוקראינה עוד הייתה חלק מהגוש הסובייטי, ניתן לשער שמתקפת סייבר הייתה דרך הפעולה המתבקשת במקרה זה, במיוחד בשל יכולתה להישען על היכרות קרובה עם המטרה מצד אחד, במקביל ליכולת ליהנות מהיתרונות של פעולה אנונימית מצד שני. היסטוריית הפעילות של האקרים לאומניים רוסיים (כגון בשנת 2007 באסטוניה ובשנת 2008 בגיאורגיה) מגבירה גם היא את הסבירות לנקיטת פעולה כזאת גם באוקראינה, או לפחות להעדפתה. למרות זאת, אין עדות ישירה למתקפות סייבר רוסיות נגד אוקראינה. יתרה מכך, למרות שדיווחים גלויים דיברו על "התכתשויות סייבר" בין גורמים פרו־בדלניים לגורמים פרו־אוקראיניים, לא נרשמה מאז יוני 2014 כל עדות לפעילות משמעותית שפגעה בתשתית קריטית אוקראינית או ביעדי פיקוד ובקרה של אוקראינה.

מלחמת האזרחים בסוריה, 2013

על פי מאמר שהתפרסם ב"ניו יורק טיימס" ב־2014, משרד ההגנה והסוכנות לביטחון לאומי של ארצות הברית פיתחו, בעקבות ההתקוממות הפנימית נגד ממשלת סוריה, תוכנית לחימה שכללה מתקפת סייבר מתוחכמת על מערכות

הפיקוד של צבא סוריה ושל הנשיא בשאר אל־אסד.[61] על פי המאמר, הנשיא אובמה דחה את התוכנית (וכן אופציות תקיפה קונבנציונלית אחרות), הן בשל ערכה האסטרטגי המוגבל והן בשל העובדה שהיכולות של נשק סייבר במהלך עימות צבאי לא נבחנו עדיין.[62] ואכן, ממשל אובמה טרם הכריע בשאלה האם נשק הסייבר הוא כלי צבאי יעיל, או שיש לשמור אותו לפעולות חשאיות בלבד.[63]

מלחמת האזרחים בלוב, 2011

ארצות הברית שקלה שימוש בנשק סייבר נגד לוב ב־2011. על פי דיווח ממקורות גלויים, המטרה הייתה לפרוץ את "חומות האש" של רשתות המחשב הממשלתיות של לוב, כדי לנתק תקשורת צבאית ולמנוע מגלאי התרעה מוקדמת לאסוף מידע ולהעבירו לסוללות טילים שהיו מכוונות נגד מטוסי נאט"ו.[64] עם זאת, ברגע שצבא ארצות הברית החליט לעבור לשימוש בכוח, הוא גם עבר להסתמך על נשק קונבנציונלי לביצוע המשימה. מאז התעורר ויכוח באשר לסיבה שמאחורי התנהלות זו (שתי סברות פופולריות היו שארצות הברית לא רצתה להפגין את יכולות הסייבר שלה ושהיא לא רצתה להיות הראשונה להשתמש בנשק סייבר למטרה זו),[65] אך ייתכן שהשאלה הרלוונטית יותר מבחינתה של ארצות הברית הייתה האם מתקפות סייבר יכולות להשיג אותה רמה של יעילות צבאית כמו מתקפות של טילים קונבנציונליים.

מסקנות וסיכום

אין חולק על כך שממשלות זרות מפתחות יכולות סייבר, בין אם כדי לחזק את מערכות איסוף המודיעין שלהן ובין אם ככלי של עוצמה מדינית. הכתיבה האקדמית והצבאית בשלוש מדינות מובילות מעידה על תמיכה בשימוש בנשק סייבר במצבי עימות, במיוחד נגד תשתיות קריטיות. ההיסטוריה עשירה באירועים שבהם הותקפו תשתיות קריטיות של האויב בעתות מלחמה משיקולים של יתרון אסטרטגי וטקטי גם יחד. סביר היה להניח שנשק מבוסס מחשב ימונף באופן דומה.

עם זאת, מרבית פעילויות הסייבר שידוע שבוצעו נגד מטרות מדיניות התרחשו במהלך תקופות של מתיחות דיפלומטית ובוצעו בעיקר על ידי גורמים לא מדינתיים, שההשערה הלא מוכחת היא כי פעלו בשליחותה של מדינה. מתקפות סייבר היו יעילות ביותר כנשק של מכה ראשונה, שנהנה מיתרון ההפתעה והאנונימיות, וזאת בשל הקושי לייחס את הפעולה ליוזם כלשהו. לעומת זאת, עימותים שבהם היה מעורב כוח צבאי (שבהם הצורך להסוות את הגורם העומד מאחוריו הוא פחות רלוונטי) עשו רק במקרים ספורים שימוש במתקפות סייבר להשגת המטרה הצבאית – בין אם כמרכיב תומך ובין אם לצורך הטעיה. במרבית

המקרים, תקיפות פיזיות היו דרך הפעולה הנבחרת, אולי משום שהן היוו חלופה אמינה ויעילה יותר.

דומה שבעתיד הנראה לעין, נשק הסייבר יתאים לפעילות חשאית ולשליחת מסרים מדיניים יותר מאשר להכרעה במלחמה ולשינוי כללי המשחק. אין בכך כדי לומר שהמצב לא ישתנה בעתיד הרחוק, אולם לשם כך יהיה על מדינות להתנסות בהפעלה ממשית של נשק הסייבר במהלך עימותים, לחוות את הבעיות שיתעוררו במהלך השימוש בו ולהפיק לקחים כדי לשפר את יעילותו. עד כה הדבר לא נעשה, כך שהשאלה "האם לנשק סייבר יש תפקיד בעימות?" נותרה על כנה. לנוכח הנטייה של צבאות לכלול טכנולוגיה בפעולותיהם, התשובה לשאלה זו היא "כן, יש תפקיד לנשק הסייבר", אלא שבשלב זה נראה שלא מדובר בתפקיד מרכזי.

הערות

1 Thomas Rid and Peter McBurney, "Cyber Weapons," *Rusi Journal*, February/March 2012, https://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf

2 *What is Critical Infrastructure?*, Department of Homeland Security, November 1, 2013, http://www.dhs.gov/what-critical-infrastructure

3 Daniel T. Kuehl, "Information Operations, Information Warfare and Computer Network Attack: Their Relationship to National Security in the Information Age," *International Law Studies*, 76 (2002).

4 DoD Directive TS3600.1," *IT Law Wiki*," http://itlaw.wikia.com/wiki/DOD_Directive_TS3600.1

5 Michael Breen and Joshua A. Geltzer, "Asymmetric Strategies as Strategies of the Strong," *Parameters*, Spring 2001, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2011spring/Breen- Geltzer.pdf

6 Shen Weiguang, "Focus of Contemporary World Military Revolution – Introduction to Information Warfare," *Jiefangjun Bao*, November 7, 1995, p. 6.

7 Major General Wang PuFeng, *The Challenge of Information Warfare*, 1995, http://fas.org/irp/world/china/docs/iw_mg_wang.htm

8 Liu Yichang, ed., *Gaojishu zhanzheng lun* (On High-Tech War) (Beijing: Military Sciences Publishing House, 1993), p. 272.

9 Deepak Sharma, "Integrated Network Electronic Warfare: China's New Concept on Information Warfare, "*Journal of Defence Studies*, 4, No. 2 (April 2010).

10 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), p. 168.

11 James C. Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, eds. James C. Mulvenon and Richard H. Yang (Washington D.C.: RAND, 1999), pp. 175-186.

12 Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," 2013 5th International Conference on Cyber Conflict (NATO: CCD COE Publications).

13 Ibid.

14 *Information Security Doctrine of the Russian Federation (2000)*, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument

15 *Russian Military Doctrine (2010)*, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf

16 Jolanta Darczewska, "The Anatomy of Russian Information Warfare," *Point of View*, 42, May 2014, http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

17 Ibid.

18 Giles and Hagestad, "Divided by a Common Language".

19 Ibid.

20 Darczewska, "The Anatomy of Russian Information Warfare".

21 *Department of Defense's Strategy for Operating in Cyberspace – July 2011*, Department of Defense, http://www.defense.gov/news/d20110714cyber.pdf.

22 *Joint Publications 3-13 Information Operations*, Department of Defense, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

23 Matthew J. Schwartz, "North Korea Behind Bank Malware, South Korea Says," *Dark Reading*, April 10, 2013, http://www.darkreading.com/attacks-and-breaches/north-korea-behind-bank-malware-south-korea-says/d/d-id/1109474?

24 Michael Mimoso, "Theories Abound on Wiper Malware Attack against South Korea," *ThreatPost*, March 21, 2013, http://threatpost.com/theories-abound-wiper-malware-attack-against-south-korea-032113/77654

25 Schwartz, "North Korea Behind Bank Malware".

26 Wiper Malware Analysis Attacking Korean Financial Sector," *Dell Secure Works*," March 21 2013, http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/

27 Sean Gallagher, "North Korean Military Blamed for Wiper Cyber Attacks against South Korea," *ArsTechnica*, April 10, 2013, http://arstechnica.com/security/2013/04/north-korean-military-blamed-for-wiper-cyber-attacks/

28 Choe Sang-Hun and John Markoff, "Cyber Attacks Jam Government and Commercial Websites in U.S. and South Korea," *The New York Times*, July 8, 2009, http://www.nytimes.com/2009/07/09/technology/09cyber.html

29 Comprehensive Nuclear Test Ban Treaty Organization, "On the CBTO's Detection in North Korea," February 12, 2013, http://www.ctbto.org/press-centre/press-releases/2013/on-the-ctbtos-detection-in-north-korea/

30 Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all

31 Ibid.

32 Kelly Jackson Higgins, "The Long Shadow of Saudi Aramco," *Dark Reading*, October 14, 2013, http://www.darkreading.com/attacks-breaches/the-long-shadow-of-saudi-aramco/d/d-id/1140664?

33 Phil Stewart, "Shamoon Virus Most Destructive Yet for Private Sector, Panetta Says," *Reuters*, October 11, 2012, http://www.reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoon-idUSBRE89B04Y20121012

34 Fahmida Y. Rashid, "Coding Errors in Shamoon Malware Suggest it may be the Work of Amateurs," *Security Week*, September 12, 2012, http://www.securityweek.com/coding-errors-shamoon-malware-suggest-it-may-be-work-amateurs

35 Paul Roberts, "Whoddunnit? Conflicting Accounts on ARAMCO Hack Underscores Difficulty of Attribution," *Naked Security*, October 30, 2012, http://nakedsecurity.sophos.com/2012/10/30/whodunnit-aramco-hack/

36 John Roberts, "Cyber Threats to Energy Security as Experienced by Saudi Arabia," *Platts*, November 27, 2012, http://blogs.platts.com/2012/11/27/virus_threats/#comments

37 Roberts, "Whoddunnit?"

38 Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back".

39 Siobhan Gorman and Julian E. Barnes, "Iran Blamed for Cyber Attacks," *The Wall Street Journal*, October 12, 2012, http://online.wsj.com/news/articles/SB10000872396390444657804578052931555576700

40 Matthew Schwartz, "Stuxnet Launched by United States and Israel," *Information Week*, June 1, 2012, http://www.reuters.com/article/2011/12/02/us-cyberattack-iran-idUSTRE7B10AV20111202

41 Ellen Nakashima, Greg Miller and Julie Tate, "U.S. Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *The Washington Post*, June 19, 2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

42 "Stuxnet Effect: Iran still Reeling," *Industrial Safety and Security Source*, August 3, 2011, http://www.isssource.com/stuxnet-affect-iran-still-reeling/

43 "Timeline of Iran's Controversial Nuclear Program," *CNN*, March 19, 2012, http://www.cnn.com/2012/03/06/world/meast/iran-timeline/

44 Max Fisher, "Nine Questions about Iran's Nuclear Program you were Afraid to Ask," *The Washington Post*, May 19, 2013, http://www.washingtonpost.com/blogs/worldviews/wp/2013/11/25/9-questions-about-irans-nuclear-program-you-were-too-embarrassed-to-ask/

45 David E. Sanger, "Obama Order Sped up Wave of Cyberattacks against Iran," *The New York Times,* June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

46 Emilio Iasiello, "Cyber Attack: A Dull Tool to Sharpen Foreign Policy", 2013 5th International Conference of Cyber Conflict, 2013, http://www.ccdcoe.org/publications/2013proceedings/d3r1s3_Iasiello.pdf

47 Council of Europe Parliamentary Assembly Resolution (2008), *The Consequences of War between Georgia and the Russian Federation*, http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=12031&Language=en

48 Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations," *Cooperative Cyber Defence Centre of Excellence*, 2010, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

49 Ibid.

50 Ibid.

51 Ibid.

52 Darczewska, "The Anatomy of Russian Information Warfare."

53 Clifford J. Levy, "Russia Prevailed on the Ground but Not in The Media," *The New York Times*, August 21, 2008, http://www.nytimes.com/2008/08/22/world/europe/22moscow.html?_r=0

54 Keir Giles, "Information Troops – A Russian Cyber Command?" 2011 3rd International Conference on Cyber Conflict (CCD COE Publications: 2011), http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf

55 Alan Greenblatt, "Israeli Bombing Ruins Gaza's Only Power Plant," *NPR*, July 29, 2014, http://www.npr.org/blogs/thetwo-way/2014/07/29/336386340/israeli-bombing-destroys-gazas-only-power-plant

56 Rick Gladstone, "Iran Blames U.S. and Israel for Spree of Cyber Attacks," *Sydney Morning Herald*, December 27, 2012, http://www.smh.com.au/it-pro/security-it/iran-blames-us-and-israel-for-spree-of-cyber-attacks-20121226-2bwa1.html

57 Ellen Nakashima and John Warrick, "Stuxnet was Work of US and Israel, Experts Say," *The Washington Post*, June 2, 2012, http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

58 John Leyden, "Israel Suspected of Hacking Syrian Air Defenses," *The Register*, October 4, 2007, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/

59 P. Polityuk, and J. Finkle, "Ukraine says Communications Hit, MPs Phones Blocked." *Reuters*, March 4, 2010, http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304

60 D. Smith, *Russia Cyberoperations* (Washington, D.C.: Potomac Institute Cyber Center, 2010), http://www.potomacinstitute.org/attachments/article/1273/Russian%20Cyber%20Operations.pdf

61 David E. Sanger, "Syria Stirs new U.S. Debate on Cyberattacks," *The New York Times*, February 25, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html

62 Ibid.

63 Ibid.

64 Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times*, October 17, 2011, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html

65 Jack Goldsmith, "Quick Thoughts on the USG's Refusal to Use Cyberattacks in Libya," *Lawfare Blog*, October 18, 2011, http://www.lawfareblog.com/2011/10/quick-thoughts-on-the-aborted-u-s-cyberattacks-on-libya/