המכון למחקרי ביטחון לאומי
מחקר אסטרטגי, חדשני ומכוון מדיניות

מבט על, גיליון 798, 16 בפברואר 2016

מתקפת סייבר נגד תשתית החשמל באוקראינה – קריאת אזהרה (נוספת)

גבי סיבוני וצבי מגן

מומחי ביטחון טוענים מזה זמן שניתן לפגוע בשירותים חיוניים, דוגמת אספקת חשמל ומים, באמצעות תקיפה במרחב הסייבר. הנחת המוצא, היא שפעולה שכזו מחייבת יכולות סייבר מודיעיניות, טכנולוגיות ומבצעיות גבוהות, ששליטה בהן מיוחסת על פי רוב למדינות המשקיעות משאבים ניכרים בפיתוחן. עד עתה, על אף הימצאותן של יכולות כאלה בידיהן, רוב המדינות הפגינו ריסון בהפעלה של כלי סייבר, שבאמצעותם יכולות היו לשבש באופן נרחב שירותים חיוניים ותשתיות קריטיות במדינות יריבות. ואולם, אירועים שהתרחשו באוקראינה באחרונה מעלים שאלה לגבי תקפו של ריסון זה. ב-23 בדצמבר 2015 דווח על אודות תקלות ברשת החשמל בחלק ממערב אוקראינה. זאת, לאחר ששובשה פעולתן של 27 תחנות חלוקה ושלוש תחנות כוח, דבר שגרם לקריסה של אספקת החשמל ובתים רבים נותקו מהרשת. לא הייתה זו הפסקת חשמל שגרתית: רשויות אוקראינה מעריכות שהגורם לתקלה היה מתקפת סייבר, שמקורה ברוסיה.

קיים קושי להוכיח באופן מידי ובוודאות מי עמד מאחורי המתקפה, אולם, ניתן להניח שעם הזמן הרשויות המוסמכות באוקראינה, בסיוע גורמים במערב, יבררו את זהותו של הגורם התוקף. משרד האנרגיה בקייב מינה ועדה שתחקור את הפרשה. לפי שעה, הערכות לגבי הגורם האחראי מתבססות על מחקר פורנזי שבוצע במחשבים שנפגעו והמראה שנעשה שימוש ברכיבים שבהם נעשה שימוש בעבר על ידי גורמים רוסיים. כך, היכולות הטכנולוגיות מצביעות, באופן שאינו מפתיע, על גורם רוסי. שירות הביטחון האוקראיני (SBU) אף האשים במפורש את רוסיה בהפסקות החשמל.

מסקנותיהן של כמה חברות אבטחה אישרו את החשד הקושר את המתקפה ל-Sandworm, שלפי חברת האבטחה iSight הנה קבוצה רוסית הפועלת בזיקה לממשלת רוסיה. זה למעלה משנה iSight עוקבת אחרי Sandworm והעלתה, כי הקבוצה אספה מידע ממחשביהם של פקידי ממשל אוקראינים, ומגורמים באיחוד האירופי ובנאט"ו. מומחי אבטחה נוספים דיווחו, כי הקבוצה התמקדה גם בתחום התקיפה של מערכות בקרה תעשייתיות. לטענת חברת האבטחה ESET, הממוקמת בברטיסלבה, התוקפים עשו שימוש בתוכנת "דלת אחורית", המאפשרת לבצע פעולות במחשבי היעד על ידי שרת שליטה מרוחק. במקרה הנדון נעשה שימוש ברכיב BlackEnergy – סוס טרויאני, שכבר ב-2014 שימש לריגול במחשבי הממשל באוקראינה, כדי לשתול תוכנה זדונית הקרויה KillDisk במחשבי תחנות כוח במערב אוקראינה.

גם השערות אשר למניע האפשרי תומכות בחשד שרוסיה היא הגורם האחראי למתקפה. אם אכן רוסיה, היא האחראית, ניתן לפרש את המתקפה כחלק מהמאבק הרוסי נגד ניתוק חצי-האי קרים, שסופח לרוסיה, מזרם החשמל שסופק עד כה מאוקראינה. לצד זאת קיים מידע רב בדבר הימצאותן של יכולות לוחמת סייבר מתקדמות בידי רוסיה וארגונים הקשורים אליה, כשרוסיה מובילה בפיתוח תפיסת לחימה, המשלבת בין פעילות במרחב הקינטי לבין זה שבמרחב הקיברנטי. תפיסת הלוחמה הרוסית כוללת מערכה תודעתית ופסיכולוגית, שביטוי לה ניתן בכל העימותים שבהם הייתה רוסיה מעורבת בשנים האחרונות, באסטוניה, בגאורגיה וכן בעימות בינה לבין אוקראינה. המעורבות הרוסית באוקראינה ידועה, הגם שהצבא הרוסי אינו מופעל בגלוי במזרח אוקראינה. פעולה במרחב הסייבר מאפשרת לרוסיה להמשיך ולהכחיש את מעורבותה באוקראינה השכנה ובה בעת להתמיד במאמצים לפגוע בה.

להפעלה אפקטיבית של נשק הסייבר נגד יעדים רגישים במדינה אחרת, ובמקרה זה באוקראינה, על רקע העימות בינה לבין רוסיה, אמורות להיות השלכות מרחיקות לכת לא רק על ניהול העימות ביניהן בהמשך הדרך, אלא גם על עימותים בין-מדינתיים נוספים או בין מדינות לבין ארגונים לא-מדינתיים, שיעלה בידם לרכוש יכולות סייבר התקפיות והגנתיות כאחד. אמנם, גם בעבר

מאת: **גבי סיבוני וצבי מגן** **מבט על**, גיליון 798, 16 בפברואר 2016

נרשמו מקרים דומים של תקיפות סייבר. אחת הדוגמאות הידועות ביותר לתקיפה של מתקני תשתית וגרימת נזק פיזי הייתה תקיפת מתקני גרעין איראניים באמצעות תכנת stuxtnet, שיוחסה לישראל ולארצות הברית. תקיפות במדינות הבלטיות, שנועדו למנוע שרות, אף הן יוחסו לרוסיה. עם זאת, מתקפת הסייבר במערב אוקראינה ביטאה שימוש מובהק בנשק זה בקנה מידה רחב, נגד תשתיות אזרחיות חיוניות. אירוע זה, המהווה תקדים של חציית "רוביקון", עלול להוות מודל לחיקוי למדינות נוספות ואולי אף לארגונים, תוך שחיקתם של גבולות הריסון שהתקיימו עד כה. יתר על כן, נראה שהאירוע באוקראינה מסמל חציית סף בעייתית במיוחד; ריגול, גניבת מידע מסחרי, פשיעה פיננסית וכן מניעת שירות – כל אלה נמצאים במרחב "נסבל", ועל אף שהם מטרידים, הם אינם פוגעים מהותית וישירות במרקם החיים. לעומת זאת, התקפה נגד תשתיות חשמל מהווה פגיעה בתשתית חיונית, שיכולות להיות לה השלכות על חיי אדם. לכן, מדובר בקפיצת מדרגה במובן ההעזה של המקור לפגיעה, ובמקרה זה המקור הוא מדינתי.

אוקראינה, כמו גם מדינות נוספות המאוימות במרחב הסייבר, תידרש לבחון כיצד לשפר את ההגנה שלה מפני אירועים דומים בעתיד. וכאן, ישראל תוכל להוות דוגמה. מדינת ישראל השכילה לפתח בעשור האחרון יכולות הגנה מתקדמות לתשתיות הקריטיות שלה. מעטפת ההנחיה ההגנתית כוללת איסוף מודיעין, ניתוחו ואספקתו לגורמים הרלוונטיים, וכן בקרה ותירגול על ידי שרות הביטחון הכללי. כך נוצרה סביבה של שיפור ושכלול מתמידים ליכולות ההגנה. עדיין, תפוצת יכולות הסייבר, המואצת בשנים האחרונות, גורמת לזליגה של יכולות מדינתיות לשחקנים חדשים-ישנים: ארגוני טרור וגורמי פשיעה. אלה נחשפים לטכנולוגיה מתקדמת ומפתחים יכולות, שנחשבו בעבר לנחלתן של מדינות בלבד. משכך מתגבר החשש, שארגונים לא-מדינתיים אלה, החסרים מנגנוני ריסון ושיקולים מדינתיים, ינסו ללכת בעקבות המודל שהציבה, למשל, המתקפה על תשתית החשמל באוקראינה.

שיבוש אספקת החשמל אינו עניין של מה בכך. די לזכור ולהזכיר את שהתרחש בישראל לפני חודשים מספר, אמנם לא כתוצאה ממתקפת סייבר אלא כתוצאה מפגע טבע: מזג אוויר חורפי קשה גרם שיבושי חשמל חמורים באזורים נרחבים ולמשך ימים ארוכים. ישראל רגישה להיבט זה במיוחד גם בשל הטיפולוגיה הריכוזית של מערך אספקת החשמל. אם כך, נדרש להמשיך ולעקוב אחר התפתחויות קשורות בסביבה האסטרטגית של ישראל ובעולם כולו, כדי להעריך האם מסתמנת מגמה של חשיפה למתקפות סייבר, העלולות לגרום נזק רב למרות ההגנה, משוכללת ככל תהייה, ולהיערך בהתאם.