



האוניברסיטה העברית בירושלים

הפקולטה למשפטים

קורס 62324- דיני סייבר ישראלים ובינלאומיים

עבודת סיום - האם תגובתו של ממשל ארצות הברית למתקפת הסייבר על חברת הבידור סוני
הולמת את הדין הבינלאומי ואת מדריך טאלין?

תוכן עניינים :

3רקע
4מתקפה מזויינת ושימוש בכוח
5פגיעה בריבונותה של ארה"ב
7חובת גילוי נאות
8דין ראוי
9סיכום
10ביוגרפיה

ב-24 בנובמבר 2014, קבוצת האקרים שהזדהתה כ"שומרי השלום" הדליפה נתונים סודיים של אולפן הסרטים של ענקית הבידור סוני שהושגו דרך מתקפת סייבר זדונית. הנתונים כללו מידע אישי על עובדי חברת סוני ובני משפחותיהם, אימיילים בין עובדים, מידע על משכורות בכירים בחברה, עותקים של סרטי סוני שלא יצאו אז, ותוכניות לסרטים עתידיים של סוני.¹ לאחר מכן, האקרים השתמשו בגרסה של תוכנה זדונית כדי לפגוע בתשתיות פיסיות של מחשבים של חברת סוני.²

במהלך הפריצה, הקבוצה דרשה מחברת סוני לבטל את פרסום סרטה "הריאיון", סרט קומדיה העוסק במזימה לרצוח את מנהיגה של צפון קוריאה, קים ג'ונג און, ואיימה בפיגועים בבתי קולנוע יבחרו להקרין את הסרט. רשתות קולנוע גדולות רבות בארה"ב בחרו שלא להקרין את סרטה לאור האיומים ולכן חברת סוני בחרה לבטל את הקרנת הבכורה הרשמית ושחררה את הסרט ישירות למהדורה דיגיטלית.³

פקידים בממשל ארה"ב הצהירו כי הם סוברים שממשלת צפון קוריאה הייתה בעלת מעורבות מרכזית בפריצה.⁴ פקידי הבית הלבן התייחסו למצב כאל "עניין רציני של ביטחון לאומי", והבולשת הפדרלית הצהירה כי הם הצליחו להוכיח את מעורבותה של ממשלת צפון קוריאה במתקפת הסייבר. ממשלת צפון קוריאה הכחישה כל קשר לפריצה ודחתה את אחריותה אליה.

תגובותיו של ממשל ארה"ב כללו מספר היבטים שונים. פחות מחודש לאחר המתקפה, צפון קוריאה איבדה את חיבורה לרשת האינטרנט.⁵ למרות שממשלת ארצות הברית לא לקחה קרדיט על פעולה זו, הנשיא דאז ברק אובמה הודיע כי ארצות הברית תבצע "תגובה פרופורציונלית" לאור הפריצה לחברת סוני.

משרד המשפטים האמריקני הוציא ב-6 בספטמבר 2018 כתב אישום רשמי לאזרח צפון קוריאני בשם פארק ג'ין-היוק על חלקו בפריצה לחברת סוני.⁶ משרד המשפטים האמריקאי טען שפארק היה האקר צפון קוריאני שעבד עבור הלשכה הכללית לסיירת המדינה ופיתח חלק מתוכנת הכופר.

¹ Gabi Siboni and David Siman-Tov, "Cyberspace Extortion: North Korea versus the United States," INSS Insight No. 646 (Dec. 23, 2014), <https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/SystemFiles/No.%20646%20-%20Gabi%20and%20Dudi%20for%20web.pdf>

² Kim Zetter, "The Sony Hackers Have Been Causing Mayhem for Years. Here's How They Did It," Wired, February 11, 2016, <https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company>

³ Sony Asks Media to Stop Covering Hacked Emails," Time, December 16, 2014, accessed December 17, 2014, <https://time.com/3633385/sony-hack-emails-media>

⁴ David E. Sanger, "U.S. Links North Korea to Sony Hacking," The New York Times, December 17, 2014, https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0

⁵ David E. Sanger, "North Korean Internet Collapses as U.S. Suspects Cyberattack," The New York Times, December 22, 2014, <https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html>

⁶ Three North Korean Military Hackers Indicted for Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes," United States Department of Justice, September 6, 2018, <https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and>

בהמשך כתב אישום זה הבשיל לתביעה שבסופה פארק חויב בסכום של 1.3 מיליארד דולר על השתתפותו במתקפות סייבר רבות המיוחסות לצפון קוריאא.

הנשיא דאז, ברק אובמה העלה בפני הקונגרס האמריקאי הצעת חקיקה לעדכן את חוק הארגונים המושחתים נוכחי כדי לאפשר לפקידי אכיפת החוק הפדרליים והלאומיים להגיב באופן טוב יותר לפשעי סייבר כמו הפריצה של סוני, וכדי להיות מסוגלים להעמיד לדין כאלה.⁷ כמו כן ממשלת ארה"ב הטילה סנקציות כלכליות על צפון קוריאא.

מקרה זה מציף שאלות רבות בדיני הסייבר הבינלאומיים. בחיבור זה אבקש לבחון האם תגובותיו של ממשל ארצות הברית למתקפת הסייבר על חברת הבידור סוני הולמות את הדין הבינלאומי ואת מדריך טאלין. בפרקים הבאים נבחן מספר אפשרויות שונות היכולות להוות בסיס משפטי לתגובותיו של ממשל ארה"ב למתקפת הסייבר שבוצעה נגד חברת סוני.

מתקפה מזוינת ושימוש בכוח.

בהתאם לסעיף 51 לאמנת האו"ם מדינה רשאית להגיב בכוח ל'מתקפה מזוינת'.⁸ במידה ומתקפת הסייבר נגד חברת סוני הינה מהווה 'מתקפה מזוינת', הרי שהמדינה המותקפת, ובנידון דינן זוהי ארצות הברית, רשאית להגיב באופן חוקי לאור כלל ההגנה עצמית.⁹

מדריך טאלין, אשר הינו ספר מלומדים המרכז את כללי המשפט הבינלאומי בתחום הסייבר אולם אינו הוראה חקוקה המחייבת מדינות, מגדיר מתקפת סייבר כך: מתקפת סייבר היא פעולת סייבר, בין אם התקפית או הגנתית, שצפויה לגרום לפגיעה או מוות לבני אדם או לנזק או הרס לאובייקטים.¹⁰ הגדרה זו מעלה שאלה פרשנית, מהו האובייקט? העמדה הסופית של מדריך טאלין היא שהקריטריון שיקבע את התשובה לשאלה זו יהיה האם המתקפה גרמה לפגיעה בפונקציונליות של המערכת שבה נמצא המידע, ובנוסף הגיעו למסקנה שאם ישנו צורך באיתחול מחדש של התוכנה, הרי שזוהי פגיעה בפונקציונליות.¹¹

מתקפת הסייבר נגד חברת סוני כללה שחרור מידע רגיש לפומבי והשמדת נתונים משמעותיים. במקרים מסוימים, אובדן הנתונים מנע מהמחשבים הנגועים והפגועים לאתחל מחדש כראוי.¹² אמנם פריצות סייבר אלו מפריעות מאוד לתפקוד החברה ובעלות נזקים כלכליים משמעותיים, אך מרבית המומחים אינם סוברים שהן עולות כדי חציית הסף של 'מתקפה מזוינת' ולכן אינן מזכות את המדינה בה החברה הותקפה באפשרות חוקית להגיב. בנוסף על כך, יש הסוברים כי זכות להגנה העצמית איננה משתרעת על התקפות של גורמים שאינם ממלכתיים אלא נגד גופים מדינתיים בלב, העצמית איננה משתרעת על התקפות של גורמים שאינם ממלכתיים אלא נגד גופים מדינתיים בלב,

Todd Spangler, "White House Unveils Proposal for Cybersecurity Information Sharing," The ⁷ Hollywood Reporter, February 13, 2015, <https://www.hollywoodreporter.com/news/politics-news/white-house-unveils-proposal-cybersecurity-763269>

United Nations Charter, art. 51 ⁸

Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 72 ⁹

Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 92 ¹⁰

Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 92 ¹¹

Kim Zetter, "The Sony Hackers Have Been Causing Mayhem for Years. Here's How They Did It," ¹² Wired, February 11, 2016, <https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company>

בעיקר אם הגופים הממשלתיים לא היו מודעים לטיב המתקפה.¹³ כך, למרות שמתקפת הסייבר יוחסה לצפון קוריאנה נראה כי בחירת אפיק זה כבסיס משפטי לתגובה נתקל בקשיים.

כמו כן, יש לבחון האם תגובותיו של ממשל ארה"ב יכול להתבסס משפטית על הפרה של סעיף 2(4) למגילת האו"ם ואיסור המשפט הבינלאומי המנהגי על שימוש בכוח על ידי מדינות.¹⁴ במדריך טאלין הפעלת שימוש בכוח במרחב הסייבר מוגדרת כך: פעולת סייבר מהווה שימוש בכוח כאשר היקף והשפעותיה דומות לפעולות שאינן סייבר העולה לרמה של שימוש בכוח.¹⁵ מדריך טאלין מציע מבחן לגבי הקריטריונים להפעלת השימוש בכוח: היקף פעולת הסייבר ותוצאותיה צריכים להיות זהים או דומים מספיק לרמה של שימוש בכוח על מנת להיחשב כפעולת שימוש כוח. על מנת לבחון את מתקפות הסייבר הזדונית לפי ולשקול האם הן תכללנה תחת האיסור לשימוש בכוח שמכוחה תקום הזכות החוקית להשתמש ביכולת להגנה עצמית עליהן לעמוד במספר תנאים. תנאים אלו הם: חומרה, מיידיות, ישירות, התערבות ופגיעה בריבונות, האפשרות למדוד את הנזק, לגיטימיות התגובה ואחריות כתוצאה מייחוס.¹⁶

קבוצת המומחים הבינלאומית שמה לב לאי הבהירות של הגדרה זו ולכך שישנם מקרים אשר אינם ברורים ולא קל לקטלגם ולהעריכם ושישנו חשש להרחבת הקריטריון האסור של שימוש בכוח על ידי מדינות. עקב חשש זה מוצע, במדריך טאלין, כי סף הגדרה המכריעה לקריטריון זה חייבת להיות חייבות להיות רגישה ביותר להערכתה הסבירה של הקהילה הבינלאומית האם במתקפת הסייבר בוצעה הפרה של האיסור על ידי המבצעים.¹⁷

נראה לא סביר שהקהילה הבינלאומית תאפיין פעולות סייבר כמו זו נגד סוני ככאלה החוצות את רף השימוש בכוח שכן תהיה זו הרחבה מהירה לאיסור זה אשר עלול לפגוע ביציבות הגלובלית וכי ישנו היסוס מוצדק כי כל שימוש בכוח סייבר יאפשר תגובה כוחנית נגדית.

נראה כי הצעידה באפיקים אלו מעלה קשיים משפטיים משמעותיים לביסוס תגובותיו של ממשל ארה"ב, ולכן יש לבחון האם מתקפת הסייבר על חברת סוני עולה כדי פגיעה בריבונותה של ארה"ב שכן מתקנים פיזיים של חברת סוני שנפגעו ממוקמים בשטחה הריבוני של ארה"ב.

פגיעה בריבונותה של ארה"ב.

נתיב משפטי נוסף אותו יש לבחון הוא האם מתקפת הסייבר נגד חברת סוני עולה כדי פגיעה בריבונותה של ארה"ב. שאלת הריבונות נידונה בהרחבה במדריך טאלין. לפי הכלל הראשון במדריך עקרון ריבונות המדינה חל במרחב הווירטואלי והקיברנטי.¹⁸ סמכות ריבונית זו חלה על תשתיות

¹³ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 72

¹⁴ United Nations Charter, art. 2(4)

¹⁵ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 69

¹⁶ United States, Department of Defense. Defense Technical Information Center. "A Framework for Creating a Cybersecurity Culture for the Internet of Things (IoT)." Technical Report, AD1018135.

¹⁷ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 69. August 2016

¹⁷ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 69

¹⁸ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 1

הסייבר, על האנשים הפועלים המרחב זה ועל כלל הפעילויות הסייבר המצויות בשטחה, זאת בכפוף להתחייבויותיה המשפטיות הבינלאומיות.¹⁹

במדריך טאלין הובע כי אסור למדינה לפעול במרחב הסייבר באופן שיפגע בריבונות של מדינה אחרת. כך ריבונות המדינה חלה על השכבות הפיזיות, לוגיסטיות והחברתיות במרחב הסייבר קיברנטי.²⁰

לפי מדריך טאלין יש למדינה המותקפת סמכות שיפוטית לעסוק במקרים בהם מתקפות הסייבר הינן בעלות השפעה בשטחה הריבוני של המדינה. הבסיס לסמכות השיפוטית הוא התכונה טריטוריאלית שהיא ביטוי או תולדה של עקרון הריבונות. ריבונות זו מזכה את המדינות בזכויות ריבוניות כגון סמכות שיפוט על תשתיות הסייבר וגם על האנשים העוסקים בפעילויות אלה.²¹ בהתאם להגדרה זו לארה"ב ריבונות על תשתיות הסייבר הקיימות במרחב הטריטוריאל של סמכות שיפוט על מתקפות הסייבר שחלו בשטחה, ולכן קיימת לארה"ב, בהתאם לטיעון משפטי זה, עילה חוקית להגיב למתקפות הסייבר הפוגעות בריבונותה.

הקריטריונים להגדרת פגיעה בריבונות מדינה על ידי מתקפת סייבר נמצאים במחלוקת. ההסכמה הרחבה היא שפעולת סייבר מפרה ריבונות כאשר התרחש נזק פיזי בתחומה הטריטוריאל של המדינה המותקפת.²² זאת בשונה מפגיעה בנתונים שאיננה בהכרח עולה כדי פגיעה בריבונות.²³

נראה כי פעולת הסייבר שבוצעה נגד חברת סוני בה נפגעו ונהרסו מחשבים ותשתיות סייבר בשטחה של מדינה אחרת תיחשב כהפרה של ריבונותה של האחרונה. כלומר, אין משמעות לכך חברת סוני היא חברה פרטית, שכן תשתית הסייבר המדוברת ממוקמת בשטח ארה"ב ולכן פגיעה זה הינה פגיעה בשלמות ריבונותה של ארה"ב. ומכיוון שכך, אם פעולת הסייבר נגד סוני מיוחסת לצפון קוריאנה, הרי שהפרה את ריבונות ארה"ב וביצעה 'מעשה בינלאומי פסול', זאת בכפוף לעמידתה בתנאים של פרק המתייחס לאחריותה של המדינה.²⁴

על מנת שמתקפת הסייבר תהווה הפרת ריבונות על הפעולה להיות מיוחסת למדינה, זאת בהתאם למשפט הבינלאומי. לאור מסקנותיה של הבולשת הפדרלית כי האקרים של צפון קוריאנה, שעובדים עבור הלשכה הכללית של הצבא, הם אלו שביצעו את המתקפה נראה שגם תנאי משפטי זה מתקיים וחל בעניינו.

הפרת ריבונות הינה 'מעשה בינלאומי פסול' מאפשר למדינה המותקפת להגיב בצעדים נגד הישות אשר הפרה את הריבונות של המדינה.²⁵ אמצעי נגד הם פעולות של מדינה פגועה המפרות חובותיה כלפי המדינה התוקפת. הזכות לנקוט באמצעי נגד כפופה למגבלות קפדניות כגון הודעה מראש, מידתיות, תזמון ואי פגיעה בזכויות אדם.²⁶ יתרה מכך, הם חלים רק נגד מדינות ולא נגד חברות או תאגידים פרטיים.

¹⁹ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 2

²⁰ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 4

²¹ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 8.

²² Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 4

²³ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 4

²⁴ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 14

²⁵ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 14

²⁶ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 22

לפיכך, במידה ונקבל את הצהרתה של הבולשת הפדרלית שפעולת הסייבר נגד סוני מיוחסת לצפון קוריאה הרי שריבונותה של ארה"ב הופרה וביכולתה להגיב באמצעים תוקפניים נגד נכסי סייבר צפון קוריאים. אם כן, יש לבחון האם תגובותיו של ממשל ארה"ב עולים בקנה אחד עם התנאים המגבילים.

נראה כי השבתת כלל חיבורה של צפון קוריאה, במידה וניתוקה מרשת האינטרנט אכן בוצעה על ידי ממשלת ארה"ב כתגובה, איננה עומדת בתנאים המשפטיים שהוצגו לעיל. אמנם פעולת הניתוק התבצעה תוך פרק זמן קצר, ובשל כך עומדת בתנאי התזמון, אולם נראה שפעולה זו איננה עומדת בתנאים האחרים הרלוונטיים בהם: הודעה מראש ומידתיות.

נראה כי כתב האישום שהוגש לאזרח צפון קוריאה, פארק ג'ין-היוק, על חלקו בפריצה לחברת סוני והעמדתו לדין עומד בתנאים המשפטיים שהוצגו לעיל. תגובה זו הינה מידתית שכן היא מכוונת כלפי אזרח אחד יחיד ולא כלפי כלל אזרחי צפון קוריאה שאינם מעורבים במתקפה. אמנם, כנראה, פארק אינו האדם היחיד שהשתתף בפעולה זו אך כל עוד ניתן לבסס את פעולותיו שלו בלבד למתקפה הרי שהוא האדם היחיד אותו ניתן להעמיד לדין. הודעה רשמית התבצעה שכן משרד המשפטים האמריקאי הודיע לצפון קוריאה על עמדתו לדין. ברם, יתכן שמסגרת הזמן נראית ארוכה שכן כתב האישום הוגש כארבע שנים לאחר מועד המתקפה, רק בשנת 2018, אך כיוון שמדובר בהעמדה תקדימית שמתייחסת למספר נוסף של מתקפות סייבר המיוחסות לפארק נראה כי פרק הזמן הארוך הינו סביר.

נראה כי אפיק זה יכול להוות תשתית משפטית חסונה וראויה לתגובותיו של ממשל ארה"ב למתקפת הסייבר נגד חברת סוני. אך לטענה משפטית שכרה בצידה שכן, כפי שיראה לקמן בפרק המתייחס לדין הראוי, התבססות על טענה זו עלול להרחיב את כמות התגובות למתקפות סייבר ואת עוצמתן לרמה שתערער על היציבות הסייבר קינטית.

ראוי לציין כי לפי ההצהרה של משרד ההגנה האמריקאי אודות המדיניות לגבי מתקפות סייבר החלות בשטחה של ארצות הברית הרי שהיא יכולה ורשאית להגיב כאשר יש פגיעה ברכוש או בחיי אדם.²⁷ כך מופיע בהצהרה "צבא ארה"ב עשוי לבצע פעולות סייבר כדי להתמודד עם מתקפה קרובה או מתמשכת נגד... האינטרסים של ארה"ב במרחב הקיברנטי. מטרת אמצעי הגנתי כזה היא להקהות התקפה ולמנוע הרס רכוש או אבדן חיים".

חובת גילוי נאות.

במידה ויהיה קשה או בלתי אפשרי להוכיח משפטית את חלקה של המדינה למתקפת הסייבר ומעורבותה בה, או במקרה דנן שמשרד המשפטים האמריקאי לא יצליח להוכיח את מעורבותה של צפון קוריאה במתקפת הסייבר, כך שהאפיק המשפטי שהוצג בפרק הקודם אינו רלוונטי, ניתן יהיה לחפש קרקע מוצקה בטענה המשפטית של חובת גילוי נאות.²⁸

United States, Department of Defense. "Department of Defense Strategy for Operating in ²⁷ Cyberspace." (Washington, DC: U.S. Government Printing Office, 2011), <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>.

²⁸ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 6

על המדינה חלה מחויבות כלפי למדינות אחרות, ובעניינינו לצפון קוריאה מחויבות כלפי כלל המדינות ובהן ארצות הברית, להבטיח שפעולות סייבר בשטחה הטריטוריאלי לא יגרמו נזק למדינות אחרות.²⁹ הפרה של חובה זו, של גילוי נאות עשויה להוות בסיס משפטי לתגובות מצד מדינות נפגעות נגד מדינות שמשטחן התבצעו פעולות סייבר זדוניות.

לפיכך, במידה ומדינה איננה עומדת במחויבותה לגילוי נאות של פעולות סייבר זדוניות היוצאות משטחה התוקפות מדינות זרות, הרי שמדינה המותקפת עשויה לנקוט באמצעי נגד שיאלצו את הראשונה לפעול להפסקת המשכן של פעולות אלו ומניעת התרחשותן העתידית. ובהשלכה למקרה דידן, אף אם לא ניתן לייחס את פעולת הסייבר המזיקה לצפון קוריאה תהיה ארצות הברית רשאית לבצע פעולות סייבר נגד צפון קוריאה, או לעסוק בצעדי נגד אחרים, על בסיס כישלונה של צפון קוריאה למלא את אחריותה לבדיקת נאותות.

מנעד אמצעי הנגדי שניתן להפעיל נגד הגורמים הלא-מדינתיים הפועלים משטחה של המדינה שכשלה במחויבותה לבדיקת הנאותות עלול להיות מורכב מתגובות בעלות עוצמות משתנות בהן אף הפרות של ריבונות המדינה המארחת.³⁰ לכן, על אף שהחוק הבינלאומי מגביל את השימוש באמצעים נגד גורמים שאינם מדינתיים לאור פעולותיהן הזדוניות, הרי שפעולות נגד המדינות שמהן הם פועלים הינן הולמות את הדין הבינלאומי.

כמו כן, כפי שצוין לעיל, רק מדינות יכולות לנקוט באמצעי נגד. לפיכך, חברת סוני לא יכולה להגיב בפעולות סייבר משלה נגד צפון קוריאה. עם זאת, גם כפי שהוצג לעיל, מדינות רשאיות לשייך פעולות סייבר התקפיות לגופים פרטיים וכאשר הן עושות זאת, המדינות נושאות באחריות משפטית לפעולות אלו לאור מחויבותן לחובת גילוי הנאותות.

דין ראוי.

בחיבור זה הוצגו מספר רב של אפיקים משפטיים דסקריפטיביים, הנעים על ספקטרום רחב המתחיל בהגדרת מתקפת הסייבר על חברת סוני כמתקפה מזויינת ועד חובת גילוי הנאות החלה על המדינה בה התקיימה המתקפה, אותם ממשלת ארצות הברית יכולה לטעון כדי לבסס משפטית את תגובותיה השונות. ברם, מתקפת סייבר זו ותגובותיה החריפות של ממשל ארה"ב מציגים אתגרים נורמטיביים אותם יש לבחון ולשקול האם הם ראויים.

חברת סוני, כפי שצוין לעיל, הינה חברה פרטית ולא מדינה ולכן הינה שחקנית שאיננה יכולה להגיב, אף אם ביכולתה יכולת הטכנולוגית לכך, נגד המתקפות הזדוניות שבוצעו נגדה. כלומר, היא הוכנסה כפיון, בעל כורחה, לזירת ההתגוששות בין ארה"ב וצפון קוריאה ששתיהן התייחסו ברצינות לפריצה זו.

צעידה באפיק המשפטי של טענת התקפה מזויינת או איום ושימוש בכוח, כפי שמופיעים במגילת האו"ם, עלולה לקבוע תקדים רדיקאלי ומסוכן. במידה ותתבצע תגובה ממלכתית אגרסיבית של

²⁹ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 6

³⁰ Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 6

המדינה המותקפת על כל מתקפת סייבר שבוצעה נגד חברה פרטית שמשרדיה נמצאים בשטחה הטריטוריאלי וריבוני הרי שהיציבות במרחב הסייבר ובמרחב הפיזי ממשי תיפגע.

בהרחבה, עצם הגדרת מתקפת הסייבר ההתקפית שבוצעה נגד חברת סוני כפגיעה בריבונותה של ארה"ב או כהפרה של חובת הנאותות, כך שהינה זכאית לפעול נגד החברה באופן חוקי עשויה לפגוע ולפרום את עקרון היציבות. אין בכך כדי לזלזל בחומרת המתקפה או בהשפעתה הכלכלית, אך למרות אלו יש חשש אמיתי כי חברות פרטיות יהפכו, או שכבר הינן חלק, ממאבקי הכוח הבין-מדינתיים ולכך משמעויות רחבות.

כמו כן, אתגר נוסף שיש לבחון את משמעותו הוא הקושי ביצירת סטנדרט אחיד וקוהרנטי שינחה את המדינות שחוו מתקפה סייבר זדונית. הצהרותיהם של נציגי ארה"ב הבהירו שהם רואים במתקפה זו אירוע משמעותי ומכונן וכי בזכותם להגיב באופן פרופורציונלי והולם. אך, מהי המשוואה לפיה ניתן לקבוע מהי התגובה ההולמת למתקפת הסייבר. האם הטלת סנקציות כלכליות הינה תגובה הולמת? האם ניתוקה המוחלט של מדינה התוקפת מרשת האינטרנט? האם הגשת כתבי אישום נגד האקרים?

מדריך טאלין פורס כללים ועקרונות מנחים, אך משאיר מקום לגמישות בתגובה זאת בכפוף למגבלות ותנאים מסוימים. לטעמי, גמישות זו הינה יתרון שכן המדינות אינן מחויבות לפעול באופן צפוי אלא באופן שיהלום את המתקפה הזדונית הספציפית הפרטיקולריות. הגמישות שהוצגה לעיל מאפשרת להכניס בתגובה שיקולים נוספים שיכולים להנחות את המדינות, כגון שיקולי הרתעה של הגוף או המדינה התוקפת או שיקולי ביטחון משמעותיים.

בשולי הדברים אוסיף כי מקרה זה מציף גם שאלות רבות נוספות אודות היותנו כלים במשחק בין גופים עוצמתיים. אילו כלים יש לחברות פרטיות, כגון חברת סוני, להתמודד עם מתקפות אלו שבוצעו על ידי מדינות? האם נגזר על חברות פרטיות להיגרר למגרש משחקים בו אין להם אפשרות להגיב? או בהרחבה של השאלה, האם אנחנו כאינדיבידואלים המשתמשים ופועלים במרחב הסייבר נידונו להיות פיונים בעל כורחנו?

סיכום

מתקפת הסייבר שכוונה נגד חברת סוני מציגה אתגרים חדשים למשפט הבינלאומי, במיוחד בהגדרת ריבונות ואחריות מדינה, וקביעת הזכות לנקוט באופן לגיטימי באמצעי נגד יעילים, לרבות הזכות להגנה עצמית. ההיענות לאתגרים החדשים הללו היא המטרה הבאה של חוק בינלאומי. המשפט הבינלאומי מתפתח עם הזמן כדי וקובע סטנדרטים חדשים של התנהגות בתחומים שעודם עדיין בחיתוליהם. לפיכך קביעת סטנדרט תקדימי כיום עשוי לעצב את התגובות העתידיות למקרים דומים.

בחיבור זה סקרנו את אופי המתקפה, את התגובות השונות של ממשל ארצות הברית, את התשתיות המשפטיות האפשריות עליהן ניתן לעמוד כדי לבסס את מעמדן החוקי של תגובות אלו. עמדנו על המורכבות הנורמטיבית של התגובות הללו ועל הקושי ביצירת סטנדרט אחיד וקוהרנטי שידריך את הקהילה הבינלאומית כיצד לנהוג כאשר מתרחשות, ויתרחשו בעתיד, מתקפות סייבר.

ביוגרפיה

חקיקה בינלאומית:

- .United Nations Charter, art. 51
- .United Nations Charter, art. 2(4)

פרשנות לחקיקה:

- .Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 72
- .Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 92
- .Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 4
- .Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 69
- .Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 1
- .Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 2
- .Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 8
- .Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 14
- .Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 22
- .Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 6

פרסומים רשמיים של ממשל ארצות הברית:

- Three North Korean Military Hackers Indicted for Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes," United States Department of Justice, September 6, 2018, <https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and>
- United States, Department of Defense. Defense Technical Information Center. "A Framework for Creating a Cybersecurity Culture for the Internet of Things (IoT)." Technical Report, AD1018135. August 2016
- United States, Department of Defense. "Department of Defense Strategy for Operating in Cyberspace." (Washington, DC: U.S. Government Printing Office, 2011), <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>

מקורות אקדמיים ופרשניים:

- Gabi Siboni and David Siman-Tov, "Cyberspace Extortion: North Korea versus the United States," INSS Insight No. 646 (Dec. 23, 2014), <https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/SystemFiles/No.%20646%20-%20Gabi%20and%20Dudi%20for%20web.pdf>

מקורות עיתונאיים:

- Kim Zetter, "The Sony Hackers Have Been Causing Mayhem for Years. Here's How They Did It," Wired, February 11, 2016,

<https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company>

Sony Asks Media to Stop Covering Hacked Emails," Time, December 16, 2014, -
accessed December 17, 2014, [https://time.com/3633385/sony-hack-emails-](https://time.com/3633385/sony-hack-emails-media)

[media](https://time.com/3633385/sony-hack-emails-media)
David E. Sanger, "U.S. Links North Korea to Sony Hacking," The New York -
Times, December 17, 2014,

https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0

David E. Sanger, "North Korean Internet Collapses as U.S. Suspects -
Cyberattack," The New York Times, December 22, 2014,

<https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html>

Todd Spangler, "White House Unveils Proposal for Cybersecurity Information -
Sharing," The Hollywood Reporter, February 13, 2015,

<https://www.hollywoodreporter.com/news/politics-news/white-house-unveils-proposal-cybersecurity-763269>