



# פעילות הסייבר של קוריאה הצפונית סקירת המצב העדכני ומבט קדימה

הראל מנשרי וגיל ברעם

ספטמבר 2020



Blavatnik Interdisciplinary  
Cyber Research Center



TEL AVIV אוניברסיטת  
UNIVERSITY תל אביב



Yuval Ne'eman Workshop  
for Science, Technology and Security  
Tel Aviv University

## הקדמה

באמצע חודש אוגוסט האחרון הודיע משרד הביטחון כי מדינה זרה, שהוערכה כקוריאה הצפונית, הוציאה לפועל תקיפות סייבר נגד עובדי התעשיות הביטחוניות בישראל. אף על פי שהתקיפה זוהתה על ידי מערך ההגנה הישראלי, ונזקיה צומצמו בהתאם, עצם ביצועה מהווה תזכורת ברורה ליכולותיה ההתקפיות של צפון קוריאה.

קוריאה הצפונית היא מדינה טוטליטרית סגורה ומבודדת, שחרף הסנקציות הבין-לאומיות המוטלות עליה הצליחה להקים מערך תקיפת סייבר מרשים והיא במרחב זה בדומה למעצמה. אף שקוריאה הצפונית אינה מוגדרת באופן רשמי כמדינת אויב, היא נמנית עם יריביה של ישראל ובמלחמת יום הכיפורים אף שלחה טייסות קרב למצרים שהשתתפו במלחמה לצידה. יכולות הסייבר ההתקפיות שלה מהוות אפוא איום שצריך ללמוד אותו ואסור להתעלם ממנו.

הסקירה להלן בנושא יכולות הסייבר של קוריאה הצפונית היא הסקירה הראשונה הרואה אור בעברית אשר דנה ביכולות הפעולה העדכניות של קוריאה הצפונית במרחב הסייבר, ומצביעה על האיום הפוטנציאלי למדינת ישראל הטמון ביכולות אלו. מחברי הסקירה, ד"ר הראל מנשרי וגב' גיל ברעם, ממליצים כי על מקבלי ההחלטות בישראל להיערך לאיום הסייבר הנשקף מקוריאה הצפונית ולגבש מסגרת פעולה לאיסוף מידע ומודיעין בהתאם.

### פרופסור יצחק בן ישראל

ראש סדנת יובל נאמן למדע, טכנולוגיה וביטחון

ראש המרכז הרב־תחומי לחקר הסייבר ע"ש בלוונטניק

## תקציר

הרפובליקה הדמוקרטית העממית של קוריאה, המכונה בפינו קוריאה הצפונית, היא מדינה שמצבה הגאופוליטי גוזר עליה מאפיינים ייחודיים – היא מבודדת ומנותקת ממרבית מדינות העולם ונתונה לסנקציות באופן תמידי. למרות זאת היא הצליחה לפתח יכולות תקיפה בלתי מבוטלות במרחב הסייבר, המאפשרות לה לתקוף מדינות רבות באסיה ובמערב בתקיפות סייבר רחבות היקף. פעולותיה נשענות על אידאולוגיה קשוחה, כמו גם על הסתגרות ובדלנות (ידידתה היחידה היא סין, וגם ידידות זו אינה יציבה). מכוני מחקר טכנולוגי מתקדמים והכשרה מוקפדת של לוחמי סייבר מקנים בסיס טכנולוגי ואקדמי חזק לפעילות הסייבר של המדינה, ומאפשרים לה לנצל את מרחב הסייבר להשגת מטרותיה: הוצאה לפועל של מבצעי סייבר התקפיים, הפצת תעמולה ושימוש בלוחמת מידע לצורכי השפעה פסיכולוגית על קהל היעד, הפצת חדשות כזב במדיה חברתית, שליחת הודעות טקסט מתחזות לטלפון למטרות השפעה ודיוג ("פישנינג") לגניבת מידע או החדרת פוגענים ועוד.

ככל הידוע, קוריאה הצפונית היא המדינה היחידה אשר משתמשת בגורמי התקיפה בסייבר גם לפשעים – גנבה ופעילויות פליליות אחרות – שנועדו להעשיר את קופת המדינה. הרווח מתקיפות במרחב הסייבר מאפשר למדינה להקצות משאבים לכרויקטים לפיתוח אמצעי הלחימה הסודיים שלה, ואגב כך – להתחמק מהסנקציות הבין-לאומיות המוטלות עליה. פעילותם של גורמי הסייבר של קוריאה הצפונית נועדה לסייע למדינה לממש את שאיפותיה בתחום הגרעין, כדי להתגונן מפני איומים מבית ומחוץ ולצמצם את בידודה משאר מדינות העולם.

בסקירה זו יוצג בסיס הידע הגלוי העדכני על גורמי הסייבר של קוריאה הצפונית על פי פרסומים מן העשור האחרון בעיקר. ננסה להציג בצורה ברורה ככל האפשר את פעילותה במרחב הסייבר של מדינה טוטליטרית סגורה – פעילות כשל מעצמה, ושמנהיגה, קים ג'ונג און, נוהג בקביעות על פי חוקי מוסר שונים בתכלית מאלו המוכרים לנו ומוכן לנקוט כל אמצעי להשגת מטרותיו, לרבות אמצעים הנחשבים בלתי חוקיים בעולם הנאור.

אף שקוריאה הצפונית אינה מוגדרת באופן רשמי כמדינת אויב, היא נמנית עם יריביה של ישראל, ובעת כתיבת שורות אלה התפרסם כי ניסתה לתקוף עובדי תעשיות ביטחוניות ישראליות, למשל; מטרתה של סקירה זו היא לזרות אור על יכולות הפעולה העדכניות של קוריאה הצפונית במרחב הסייבר ולהצביע על האיום הפוטנציאלי למדינת ישראל הטמון ביכולות אלו.

## פעילות הסייבר של קוריאה הצפונית – מגבלות הידע והמחקר

המידע המודיעיני הגלוי על קוריאה הצפונית הוא מידע היסטורי, שאינו משקף במדויק את יכולותיו הנוכחיות של המשטר. מקורו של רוב המידע העדכני על המדינה בדו"חות מודיעין של ארצות הברית וקוריאה הדרומית, ושאר המידע מתקבל מחברות סייבר ואבטחת מידע, אולם גם ממסמכים אלה מושמטים פרטים, ככל הנראה מטעמים ביטחוניים. נוסף על כך, תשתית האינטרנט הבעייתית של קוריאה הצפונית והשליטה הקפדנית של המשטר בשימוש במרחב הסייבר במדינה סגורה זו מקשים מאוד על ניטור מודיעיני של תשתיות הסייבר שלה. מהימנותם של הדיווחים מקוריאה הדרומית אינה ברורה – הם עלולים להיות מעוותים, בשל הסכסוך המתמשך בין המדינות וכן בשל הבדלי התרבות ביניהן. לא זו אף זו, רוב דו"חות אבטחת הסייבר שמפרסמות חברות אבטחת המידע עוסקים בעיקר בפן הטכני של התקיפות ומתמקדים פחות במצב הבין-לאומי ובאינטרסים שגורמים לתקיפה.

לאור כל אלה, ייתכן כי המידע המצוי בדינו על קוריאה הצפונית אינו מספק למעשה תמונה מלאה על יכולות הסייבר של המדינה. אולם לאור ניסיונותיה של קוריאה הצפונית לפעול גם מול מטרות בישראל (ראו פירוט בהמשך) אנו רואים חשיבות רבה בהצגת המידע העדכני הקיים ובהצבעה על הצורך להפנות את תשומת ליבם של מקבלי ההחלטות בישראל לנושא.

## רקע

כדי להבין את פעילותה ההתקפית של קוריאה הצפונית במרחב הסייבר חשוב להזכיר תחילה שתי תפיסות עיקריות אשר עומדות ביסוד מניעיו של המשטר ומשמשות בסיס לפעולתו: פילוסופיית "ההסתמכות העצמית" (ג'וצ'ה, Juche) ודוקטרינת "הצבא ראשון" (סונגון, Songun).

ג'וצ'ה היא הפילוסופיה הלאומית של קוריאה הצפונית והאידיאולוגיה הפוליטית הרשמית של המדינה. אידיאולוגיה זו גובשה ב-1955 בתקופת שלטונו של "המנהיג הדגול", שליטה הראשון של הרפובליקה קים איל-סונג (Kim Il-Sung), ומאז התקבעה והפכה לדוקטרינה מחייבת. היא מדגישה את הצורך בעצמאות שתושג באמצעות הישענות עצמית, אחדות כוחות, הגנה עצמית ואחריות מוחלטת לפתרון בעיות המדינה. לאידיאולוגיה זו יש השפעה רבה על מושגי הריבונות הלאומית והעצמאות של קוריאה הצפונית, ולמעשה מדובר בתחושת בוז כלפי השפעות תרבותיות ופוליטיות חיצוניות. אידיאולוגיה זו מקדשת את העצמאות והריבונות של אזרחי קוריאה הצפונית וקוראת להם להיות אדונים לגורלם ולא להיות תלויים בכוחות חיצוניים או נתונים לחסדיהם (Person, 2014; Terry & Wood, 2015) היא מתבטאת בכל ההיבטים בחייהם של האזרחים, מפוליטיקה וכלכלה דרך חינוך ותרבות צריכה ועד ביטחון.

דוקטרינת סונגון מבטאת את התפיסה כי הצבא חיוני לשימור המשטר; על פיה, בעת הקצאת משאבי המדינה תהיה לצבא ולכוחות הביטחון עדיפות על פני עניינים פוליטיים, כלכליים ואחרים. הדוקטרינה מעוגנת בסעיף 58 בחוקה, שבו נקבע כי על המדינה להתבסס על מערכת הביטחון הארצית – הכוללת את כל אזרחי המדינה.

צבאה הסדיר של קוריאה הצפונית הוא אחד הצבאות הגדולים בעולם, ומספר החיילים בו עולה על שליש מאוכלוסיית המדינה (25 מיליון איש) – יותר ממיליון חיילים בשירות סדיר ו-7.7 מיליון אנשי מילואים (Kim, 2015). הצבא מצויד בכלי נשק קונבנציונליים שמספרם רב ביחס לשטחה של המדינה ולגודל אוכלוסייתה. על פי נתונים משנת 2020, בארסנל היבשתי של קוריאה הצפונית יש 6,045 טנקים, 10,000 כלי רכב משוריינים וארטילריית שדה של 800 תותחים מתנייעים, 1,000 תותחים נגררים ו-2,110 משגרי רקטות. לחיל הים 83 צוללות, 416 ספינות סוור, כ-40 ספינות קרב ו-260 כלי נחיתה אמפיביים. לחיל האוויר 458 מטוסי קרב, 114 מפציצים כבדים, 224 מסוקים (מהם 20 מסוקי תקיפה), 169 מטוסי אימון וארבעה מטוסי תובלה (Global Firepower, 2020). על מספר הטילים הבליסטיים שברשות המדינה אין מידע מדויק.

למרות מספרם הרב של אמצעי הלחימה המצויים ברשות המדינה, אין לצבא מספיק אמצעים לתחזק אותם בשל משטר הסנקציות שקוריאה הצפונית נתונה בו מאז הוטל בידי מועצת הביטחון ב-2006; המחסור בדלק, חשמל ומזון בעקבות הסנקציות פוגע גם ביכולות הצבא לפרוס את כוחותיו במהירות ולהתמודד עם לחימה ממושכת. מכל האמור עד כה אפשר להבין כי בהחלטותיו אילו יכולות לפתח מונע המשטר בקוריאה הצפונית בעיקר מצורך ומכורח.

בשל אופיה הריכוזי והסגור של המדינה, מבנה מערכת קבלת ההחלטות בקוריאה הצפונית אינו ידוע. עם זאת, ברור כי הקובע הוא המנהיג קים ג'ונג-און (Kim Jong-un) – שעלה לשלטון בדצמבר 2011 – והוא ככל הנראה מי שמגדיר את יעדיהם של גופי המודיעין. להבנתנו, לשירותי המודיעין של קוריאה הצפונית שלושה יעדים עיקריים: לשמור על קיום המשטר והמפלגה ולהגן על המנהיג ובני משפחתו; לאסוף מודיעין ולבצע פעולות חשאיות במדינות אויב – בעיקר בארצות הברית, בקוריאה הדרומית ובין; ליזום מבצעים שימלאו את קופת המדינה. עד כה, עיקר המשימות של שירותי המודיעין כללו איסוף מידע ומודיעין על סיכונים פוליטיים, צבאיים או כלכליים למשטר וליציבותו ועל טכנולוגיות צבאיות ואזרחיות, סיוע למימוש יעדי מדיניות החוץ של המשטר, תמיכה בארגוני מהפכה ובארגוני טרור זרים והכשרת חבריהם ורכישה – או גנבה – של הון זר למימון פעולות המודיעין והמדינה.

## תחום הסייבר

על פי אסטרטגיית הסייבר של קוריאה הצפונית, הנשענת על ג'וצ'ה וסונגון, מרחב הסייבר נתפס כמרחב המאפשר לנהל מערכה ממושכת מול גורמים חזקים ובעלי יתרון טכנולוגי. השימוש במבצעי סייבר תואם את האסטרטגיה הלאומית של שימוש בטקטיקות לוחמה א-סימטריות כדי לפגוע באויבי המדינה. הקושי לייחס תקיפה במרחב הסייבר לגורם מסוים מקל על התוקף להכחיש את המעורבות בה; לפיכך, שימוש בתקיפות במרחב הסייבר מסייע לקוריאה הצפונית לצמצם את הסיכוי לפעולת תגובה נגדה, ושימוש במרחב של בעלות בריתה (בעיקר סין) מאפשר למנוע את ייחוס התקיפות לה. גם חוסר היציבות הביטחונית בחצי האי הקוריאני תורם להעדפת השימוש בתקיפות סייבר – תקיפה צבאית ישירה של קוריאה הדרומית או של מדינה אחרת עלולה להוביל למתקפת תגובה על קוריאה הצפונית, וזו עלולה להסלים לעימות צבאי נרחב ולפגוע במשטר. לעומתה, התקפה במרחב הסייבר עשויה להשיג תוצאות טובות לא פחות, ואילו הסיכוי לתגובה לה נמוך יותר.<sup>2</sup>

בתחילת שנות התשעים, לאור לקחי מלחמת המפרץ בעניין השימוש בלוחמת מידע, פיתח מנהיג קוריאה הצפונית אז, קים ג'ונג-איל (Kim Jong-il), בנו של קים איל-סונג ואביו של קים ג'ונג-און – מנהיגה של קוריאה הצפונית כיום), תוכנית סייבר שהתבססה על אידאולוגיית ההסתמכות העצמית (Boo, 2017). כבר אז ביטאה התוכנית את ההבנה כי מרחב הסייבר עשוי להעניק לקוריאה הצפונית יכולות הגנה והתקפה טובות לצד אלה הקינטיות, ואלה יאפשרו לה לממש את מטרותיה ולייצר הרתעה. בשנת 2015 פרסם המרכז האמריקני ללימודים אסטרטגיים בין-לאומיים (CSIS) את הערכתו כי קוריאה הצפונית תמשיך לייחס ערך אסטרטגי לפעולותיה

1 פעמים רבות קשה להצביע על מקור התקיפה ולייחס אותה לתוקף מסוים; בעיה זו מכונה "בעיית הייחוס" (attribution problem), ומתעוררת כאשר הנתקף זיהה את עצם התקיפה אך טרם זיהה את התוקף. ההשפעה המיידית של מצב כזה היא חוסר ודאות באשר לכוונותיו של התוקף ואי-בהירות בעניין מידת ההיתכנות של תגובת נגד והרצון לבחור באופן פעולה זה. להרחבה בעניין זה ראו: Lindsay, 2015, וכן: Rid & Buchanan, 2015.

בעיית הייחוס גוברת בתחום הביטחוני, שם נפוצה מאוד יכולת ההכחשה (plausible deniability); ההכחשה מאפשרת למנהיגים להמשיך לפעול בהתאם לתפיסת עולמם, ובה בעת להגן על המוניטין שלהם ועל אמינות פעולותיהם בטענה שלא היו מודעים לפעולות שהתרחשו – אם פעולות אלה לא צלחו. אף שאין זו תופעה חדשה, עד כה היה הדיון בהכחשות של פעולות התקיפות במרחב הסייבר מצומצם למדי. להרחבה בעניין זה ראו: Poznansky, 2020.

2 להרחבה על אסטרטגיות של מדינות בעת עימות במרחב הסייבר ראו: Baram & Sommer, 2019.

במרחב הסייבר ולהעמיק את שילובן בכוח הצבאי הקונבנציונלי (Jun, LaFoy, & Sohn, 2016). כדי שיתאפשר למדינה לשפר את יכולותיה הטכנולוגיות, מערכת החינוך של קוריאה הצפונית שמה דגש רב בלימודי מתמטיקה, ומעניקה לאומה אמן במפתחים, בקריפטוגרפים ובחוקרי אבטחה (Fisher, 2013; Jaewon, 2017).

כיום, יכולות ההתקפה וההגנה של קוריאה הצפונית במרחב הסייבר מבוססות על יחידות סייבר מתקדמות ומתוחכמות ועל שימוש ברכיבי לוחמה אלקטרונית כגון ניטור לוויינים, חסימת GPS, דופק אלקטרומגנטי (EMP) ועוד. בלחימה במרחב זה נשענת קוריאה הצפונית על איסוף מודיעין גלוי (OSINT) ועל רגולציה של הרשת בתחומי המדינה (Mercado, 2004). גורמי התקיפה של קוריאה הצפונית גורמים בשיטתיות נזקים לחלק ניכר מקורבנותיהם – הם משתמשים בכלי לשליטה מרחוק (RAT) כדי למפות את הרשת שבה הם נמצאים, לאתר משתמשים מרכזיים ולהתקין במחשביהם כלי שהורס אותם לחלוטין.

המשטר בקוריאה הצפונית מעוניין למקסם את הרווח שמפק מיכולות הסייבר של המדינה (Fisher, 2013), ולהשתמש בו כדי לממן פיתוח כלכלי ופיתוח של יכולות הגרעין (מדיניות המכונה בקוריאה הצפונית Byungjin). על פי הדו"ח החצי שנתי שהוגש לוועדת הסנקציות של מועצת הביטחון של האו"ם בקיץ 2019, קוריאה הצפונית ממשיכה לפתח נשק להשמדה המונית; למימון הפעילות היא יוזמת פריצות לבנקים וגנבת מטבעות קריפטו (crypto currencies) ומשתמשת במרחב הסייבר כדי להלבין את הכסף שנגנב. פעולות אלה של לוחמי הסייבר של המדינה – מרביתם אנשי המודיעין הצבאי (ה-RGB; ראו פירוט בהמשך) – הניבו לקוריאה הצפונית לפחות שני מיליארד דולר. מומחי האו"ם הבהירו כי פריצות לאתרי סחר במטבעות קריפטו אפשרו לקוריאה הצפונית להזרים לקופתה כספים בדרך שקשה יותר לעקוב אחריה, ואשר נתונה לפיקוח ממשלתי מצומצם יותר מאשר מגזר הבנקאות המסורתי (Nichols, 2019).

קים הואנג-קוונג (Kim Heung-kwang), פרופ' למדעי המחשב שערך בשנת 2003 מקוריאה הצפונית לסין וממנה לקוריאה הדרומית, מבהיר כי קוריאה הצפונית מסוגלת להוציא לפועל מתקפות סייבר מתוחכמות שרמתן הטכנולוגית גבוהה. לפי עדותו, בין 10 ל-20 אחוזים מהתקציב הצבאי של המדינה מוקדשים לפעולות במרחב הסייבר, וקוריאה הצפונית תוקפת מדינות אחרות כדי להמחיש את יכולותיה; תקיפות סייבר אלה עלולות להוביל לתקיפות צבאיות, להרג אנשים ולהרס ערים (Chanlett-Avery, Rosen, Rollins, & Theohary, 2017).

לדברי הואנג-קוונג, המשטר מתמקד בהרחבת יכולות לוחמת הסייבר שלו מכמה מניעים: בראש ובראשונה, יכולות סייבר הן דרך חסכונית להתגבר על הקשיים הטמונים בלוחמה קינטית; בלוחמה המודרנית, ביכולות הסייבר טמון פוטנציאל רב יותר להגן על המשטר לאורך זמן מזה של ארטילריה כבדה או מטוסים. נוסף על כך, לוחמת סייבר מקנה לקוריאה הצפונית יתרון אסטרטגי, משום שהיא מאפשרת למדינה לתקוף אחרים ובד בבד להגביל את היכולת לתקוף אותה – בידול רשתותיה מרשת האינטרנט העולמית מאפשר לה לנצל לטובתה את הפגמים המובנים של האינטרנט לצורכי התקפה מבלי לפגוע בהגנתה.

חלק ניכר מכלי התקיפה והיכולות של קוריאה הצפונית נבנו מהיסוד, תוכננו ותוכנתו ללא הסתמכות על כלים קיימים או מסחריים. הם מתאפיינים לעיתים קרובות בהצפנה חזקה, בשיטות הסוואה וכיסוי מתוחכמות ובמנגנון השמדה עצמית מתוחכם. ייחודיותם של כלים אלו מציבה פעמים רבות אתגר בפני מערכות הגנה, שכן לא פעם נעשה שימוש ביכולות מפותחות יותר

מהנדרש. עם זאת, דווקא מאפיינים מקלים לעיתים את היכולת לייחס את התקיפה לקוריאה הצפונית (למשל בתקיפה של קוריאה הדרומית וארצות הברית בשנת 2006, שתתואר להלן).

במובן זה, היכולות והכלים המתקדמים והייחודיים שמפתחת קוריאה הצפונית הם עבורה לא רק נקודת חוזק, כי אם גם נקודת חולשה – משום שחשיפתם עלולה לגרום לה לכגיעה רחבת. זוהי חולשה שאפשר לנצלה כדי להתמודד עם תקיפות מצד המדינה (כהן, 2017). כדי להתמודד עם חולשה זו מפתחים גורמי התקיפה של קוריאה הצפונית מנגנונים מתקדמים שיאפשרו להתחמק מרכיבי הגנה ברשת בלי לשנות את המתווה המבצעי, כגון הצפת התקשורת בין הכלים לשרתי התקיפה או "עטיפת" הכלי בקוד מיותר ליצירת חתימה שונה שתוכנות אבטחה לא יזהו ולכן לא יסרקו.

## התשתיות התומכות במערך הסייבר של קוריאה הצפונית (חינוך, טכנולוגיה ותקשורת)

ביולי 2014 פרסם מכון המחקר Yonhap שבקוריאה הדרומית כי בקוריאה הצפונית מועסקים כ-5900 אנשי תקיפת סייבר (Cook, 2015; DeSimone & Horton, 2017). כדי שיתאפשר לגייס את הלוחמים המתאימים ביותר, נעשים מאמצים לאתר ילדים בעלי כישרון מתמטי כבר במסגרות החינוך בבתי הספר היסודיים; הם נשלחים להכשרה מתקדמת וקפדנית בתחומי מדע וטכנולוגיה, ובהמשך גם ללימודי שפות זרות. התלמידים המוצלחים מהם נשלחים לאוניברסיטת קים איל סונג (Kim Il-Sung University), לאוניברסיטת קים צ'אק לטכנולוגיה (Kim-Chaek University of Technology) או לאוניברסיטה לפיקוד אוטומציה (Command Automation University) (Kovacich & Jones, 2016), והסטודנטים המצטיינים נבחרים לשרת בגופי לוחמת הסייבר.

לוחמי הסייבר משתתפים בתוכנית לימודים אינטנסיבית ומואצת, וחלקם אף נשלחים ללימודים ברוסיה או בסין. הסטודנטים ולוחמי הסייבר המצטיינים זוכים לתמריצים מיוחדים; כך, לדוגמה, הורים לסטודנטים שסיימו את תוכנית הסייבר בציונים מעולים זוכים להזדמנות לעבור לחיות בבירה פיונגיאנג (Pyongyang), ולוחמי סייבר נשואים זוכים לדיוור, קצבת מזון ומלגות. כמו כן, מתוקף תפקידם יש ללוחמי הסייבר גישה לאינטרנט העולמי.

בשל מאפייני תשתית התקשורת נאלצים גורמי הסייבר של קוריאה הצפונית להשתמש בשרתים ובכתובות IP בסין, במלזיה ובמדינות נוספות בדרום-מזרח אסיה כדי לבצע פעולות תקיפה נרחבות. לכאורה, החברה האחראית לתקשורת האינטרנט החיצונית של קוריאה הצפונית היא Star Joint Venture Co, חברה שהקימה חברת הדואר והתקשורת בשיתוף Loxley Pacific בתאילנד (Gilbert, 2015); אולם קיימות עדויות כי תקשורת האינטרנט החיצונית של המדינה מנותבת באמצעות חברת התקשורת הסינית China Unicom. בחודש פברואר 2014 הסכימו קוריאה הצפונית וקוריאה הדרומית להרחיב את הגישה לאינטרנט העולמי גם לחלקה של קוריאה הצפונית באזור התעשייתי המשותף קסונג (Kaesong), הצמוד לגבול בין המדינות.

רשת החשמל של קוריאה הצפונית אינה מסוגלת לספק תשתית נרחבת דיה לכלל האוכלוסייה, ולפיכך האזרחים מקבלים חשמל בקיצוב. היעדרה של אספקת חשמל קבועה פוגעת בין השאר ביכולת להשתמש בתקשורת הסלולרית במדינה. בקוריאה הצפונית רשת סלולר אחת, קוריולינק (Koryolink), אשר נשלטת היטב בידי המשטר ואינה מאפשרת גישה לאינטרנט

חיצוני. על פי הסטטיסטיקה הרשמית של המדינה, בתחילת 2019 היו במדינה כחמישה מיליון טלפונים סלולריים; כשני שלישים מאוכלוסיית המדינה משתמשים בטלפון סלולרי, ובבעלות של משפחות רבות יש מחשב אישי (Williams, 2019).

תשתית התקשורת של קוריאה הצפונית מחולקת לשני חלקים עיקריים: האחד הוא חיבור לרשת האינטרנט העולמית, והאחר – רשת אינטראנט בשליטת המשטר, המכונה קוואנגמיונג (Kwangmyong), ובה שירותי דוא"ל ואתרים שונים (כמה אתרים מהאינטרנט העולמי שהוחלט כי הם תורמים למדע ולטכנולוגיה, והועלו לרשת לאחר שעברו צנזורה ונבדק כי אין בהם מידע מזיק, והשאר – אתרים מקומיים); רשת האינטראנט מקשרת בין מוסדות בתוך המדינה ואינה מחוברת לרשת האינטרנט העולמית. לאזרחים זרים אשר מגיעים למדינה מתאפשרת בדרך כלל גישה לאינטרנט; לעומת זאת לאזרחי המדינה מותרת גישה רק לרשת האינטראנט – רק לגורמים נבחרים מתאפשר להתחבר לאינטרנט החיצוני, והם נתונים לפיקוח הדוק מחשש לפעילות נגד המשטר. לפי דיווחים של עריקים (יוצאי צבא ואזרחים) אפשר ככל הנראה לעקוף חלק ניכר ממחסומי הצנזורה הטכנולוגיים של קוריאה הצפונית ולקבל גישה לרשת, אך הדבר כרוך בסיכון המשתמש.

כחלק ממאמצי השלטון לשמור על עצמו ולפקח על אזרחי המדינה, הוא פועל לניטור המשתמשים באינטרנט ולפיקוח עליהם. לשם כך פותחה בקוריאה הצפונית מערכת ההפעלה הייחודית "כוכב אדום", המשמשת לניטור טלפונים סלולריים ומחשבים. המשטר מחייב את כלל אזרחי המדינה להשתמש במערכת זו (North Korea's 'paranoid' computer operating system revealed, 2015). נראה שבתחילת 2019 הצליחו השלטונות להתקין מערכת הפעלה זו בכל המכשירים הסלולריים, וכיום היא מותקנת בכל מכשירי הטלפון הסלולרי ומחשבי הלוח (הטבלטים) הנמכרים. ככל הידוע, התוכנה עדיין אינה מותקנת בחלק מן המחשבים האישיים – ובעיקר במחשבים ניידים. נוסף על כך, בידי מערך ביטחון הפנים והמשטרה בקוריאה הצפונית מוחזקות רשומות של כלל המחשבים במדינה, ויחידה 109 של המשטרה אמונה על ניטור המשתמשים בהם ופיקוח עליהם, בין השאר במסגרת "ביקורי בית".

מערכת ההפעלה הייחודית "כוכב אדום" אינה מאפשרת למשתמש לפתוח קובצי טקסט או מדיה שהגיעו ממקור שאינו ידוע או מוכר למשטר; המערכת תאפשר להשתמש רק בדפדפן שייצרה המדינה ולפתוח רק קובץ שנושא חתימה דיגיטלית ייעודית שאישר המשטר, המעידה על כך שהופק על ידי מקור מוסמך. המערכת מצלמת את מסכי המשתמשים, שומרת את תצלומי המסך במאגר למשך זמן ומעניקה למערך ביטחון הפנים גישה אליהם. המשתמש אינו יכול למחוק את הצילומים הללו או את היסטוריית הפעילות והגלישה שלו.

## שיתופי פעולה בין-לאומיים בתחום הסייבר

קוריאה הצפונית נסמכת מאוד על טכנולוגיות סיניות ועל סיוע במשאבים מסין. בין השאר סיפקה לה סין תוכניות לימודים בתחום הסייבר ומערכות חומרה. חלק מלוחמי הסייבר של קוריאה הצפונית מתאמנים בסין, ובסיס סייבר של המדינה מצוי בשטח סין.

## **משרד הכוחות המזוינים (MPAF – Ministry of People's Armed Forces)**

משרד הכוחות המזוינים מופקד על צבא קוריאה הצפונית (KPA) ומפקח על מחלקת המטה הכללי (GSD) (Office of the Secretary of Defense, 2015).

## **צבא קוריאה הצפונית (KPA – Korean People's Army)**

הצבא הוא הגוף האחראי לתכנון המבצעים. היקף כוחות הסייבר של קוריאה הצפונית מוערך בכ-3000 עד 6000 האקרים, ומרביתם שייכים למחלקת המטה הכללי בצבא ולסוכנות הביון הצבאית של המדינה (RGB, ראו להלן). ייתכן שיחידות הסייבר בצבא משתפות פעולה עם סוכנות הביון.

## **מחלקת המטה הכללי (GSD – General Staff Department)**

מחלקת המטה הכללי אחראית לפיקוד המבצעי ולפעילות מבצעית, ממונה על הכוחות המזוינים של קוריאה הצפונית ועל תכנון פעילותם וניהולה ומפקחת על סוכנות הביון הצבאית (RGB).

## **סוכנות הביון הצבאית (RGB – Reconnaissance General Bureau)**

סוכנות הביון הצבאית של קוריאה הצפונית, הידועה גם כיחידה 586, עוסקת במודיעין מסורתי, במבצעים מיוחדים ובסייבר, ובכלל זה בהפעלת סוכנים בחו"ל. היא מפעילה כמה יחידות ולשכות אשר מתמחות בתחומים שונים: מבצעים מיוחדים, מודיעין קרבי, מעקב ותצפית, תקיפות סייבר, טכנולוגיה, איסוף מודיעין בחו"ל ומגעים עם קוריאה הדרומית (Office of the Secretary of Defense, 2015).

סוכנות הביון – ובייחוד יחידה 121 שלה (לפירוט ראו בהמשך) – היא הגוף שמנהל את מבצעי הסייבר. הסוכנות היא ככל הנראה החממה המרכזית בקוריאה הצפונית לטיפוחם של מבצעים סודיים, ואחראית לחלק ניכר מפעולות הטרור של קוריאה הצפונית; היא הואשמה בתקיפות שונות גם מחוץ למרחב הסייבר, כגון הטבעת ספינת המלחמה של קוריאה הדרומית Cheonan בשנת 2010. אפשר שהסוכנות אף מכוונית את פעולתם של ארגוני האקרים המציגים עצמם כארגונים עצמאיים, אך למעשה פועלים בחסות המדינה. ההאקרים שמעסיקה הסוכנות מתגוררים לעיתים מחוץ למדינה, כדי לנצל את התשתיות המתקדמות של המדינות שבהן הם מוצבים (Chanlett-Avery, Rosen, Rollins & Theohary, 2017).

אלה יחידות הסוכנות שזוהו: לשכה 1 – מבצעים; לשכה 2 – מעקב ותצפית; לשכה 3 – מודיעין; לשכה 5 – דיאלוג פנים-קוריאני; לשכה 6 – טכנולוגיה; לשכה 7 – שירותים עורפיים (Lankov, 2017). על לשכה 4 אין מידע, אולם על דרך האלימינציה ייתכן כי זו הלשכה המפעילה את גורמי הסייבר של הסוכנות.

ידוע על כמה יחידות סייבר ומערכי תקיפה השייכים לסוכנות הביון:

יחידה 91 – אחראית לפריצה למחשבים ולכתיבת תוכנה ליחידות הסייבר של הארגון. היחידה ממוקמת במחוז מנגיונגדה (Mangkyungdae) באזור פיונגיאנג, ופועלים בה כמה אנשים (Ji Young, Jong In, & Kyoung Gon, 2019).

יחידה 121 – מורכבת מגורמי מודיעין לצד גורמי תקיפה. מפקדת היחידה ממוקמת במחוז מונשינדונג (Moonshin-dong) שבאזור פיונגיאנג, סמוך לנהר טאדונג (Taedong). חלק מגורמי היחידה פועלים מתוך סין – אחת ממפקדות היחידה מצויה במלון צ'ילבוסאן (Chilbosan) בשניאנג (Shenyang), בירת מחוז ליאונינג (Liaoning) שבסין, סמוך לגבול עם קוריאה הצפונית.

כמו סין, גם רוסיה מספקת משאבים טכנולוגיים לקוריאה הצפונית. לוחמי סייבר של המדינה הוכשרו בלוחמה אלקטרונית ברוסיה, ובין השאר ככל הנראה גם למדו שם להשתמש בטכנולוגיה של דופק אלקטרומגנטי. מרצים מובילים בתחום הסייבר, בוגרי האקדמיה הצבאית המרכזית של הצבא האדום על שם מיכאיל פרונזה (Frunze Military Academy), השתתפו בהדרכות בתחום הסייבר בקוריאה הצפונית.

קוריאה הצפונית מקיימת קשרים ארוכי טווח גם עם איראן; היא סיפקה למדינה השיעית אמצעי לחימה מתקדמים מתוצרתה, ובכלל זה טכנולוגיות לפיתוח טילים וגרעין וכן טכנולוגיות סייבר, והיא מכשירה אנשי סייבר איראנים. בשנת 2012 חתמו קוריאה הצפונית ואיראן על מזכר הבנות טכנולוגי שמטרתו לסייע במאבק נגד "אויבים משותפים" במרחב הסייבר, ובו הסכימו על שיתוף פעולה במחקר, חילופי סטודנטים ומעבדות משותפות. בפרויקטים משותפים של קוריאה הצפונית ואיראן הועבר בין המדינות מידע בנושאי טכנולוגיות מידע (IT), הנדסה, ביוטכנולוגיה, אנרגיה מתחדשת וקיימות (Park, 2016).

קוריאה הצפונית מקיימת קשרים ביטחוניים גם עם משטרו של הנשיא אסד ומספקת לו אמצעי לחימה שונים. הכור הגרעיני הסורי הוקם בדיר א-זור בסיוע קוריאה הצפונית, ופורסם כי אנשי סייבר סורים עוברים הכשרה בקוריאה הצפונית (Ramani, 2018).

## **ארגונים בקוריאה הצפונית העוסקים בסייבר**

### **הוועדה לענייני המדינה (SAC – State Affairs Commission)**

ה-SAC היא הגוף החזק ביותר בקוריאה הצפונית; בראשה עומד המנהיג, והיא קובעת את המדיניות (Socialist constitution of the Democratic People's Republic of Korea, 2017, §106). עד שנת 2016 עמדה בראש מדרג המבנה הביטחוני במדינה ועדת ההגנה הלאומית (NDC – National Defense Commission), אשר פיקחה על כמה גופי ביטחון ומודיעין ובהם משרד ההגנה, המשרד לביטחון העם (MPS), משרד הכוחות המזוינים (MPAF), צבא קוריאה הצפונית (KPA) והמחלקה לביטחון המדינה (Office of the Secretary of Defense) (MSS) (2015). מטרתה העיקרית של החלפת ה-NDC ב-SAC הייתה לחזק את מעמדו של קים כשליט המדינה (פיפילד, 2020).

### **המחלקה לביטחון המדינה (MSS – Ministry of State Security)**

המחלקה לביטחון המדינה – שירות המודיעין הראשי של קוריאה הצפונית – כפופה ישירות למנהיג ונתונה לפיקוח ה-NDC. היא אחראית לפעולות ריגול בחו"ל, לסיכול של ריגול נגדי, לפיקוח על מחנות שבויים ולתפיסת עריקים, ועוסקת גם בסיגניט ובתקיפות סייבר (Office of the Secretary of Defense, 2015).

### **המשרד לביטחון העם (MPS – Ministry of Public Security)**

המשרד לביטחון העם ידוע גם כמשרד לאבטחה ציבורית; הוא אחראי לכוח המשטרה הלאומי של קוריאה הצפונית, לסדר המקומי, לחקירות פליליות ועוד.

יחידה 121 ומעבדה 110 אחראיות לאיסוף טכנולוגי של מודיעין ולהטמנת כלי תקיפה באמצעות חדירה לרשתות מחשבים. יחידה 121 מבצעת תקיפות סייבר, פעולות ריגול וכשעי מחשב בעיקר נגד קוריאה הדרומית, ארצות הברית ויפן. היחידה הייתה אחראית למבצעי פריצה לארגונים גדולים ופעילותה מוכרת לסוכנויות מודיעין ולחברות אבטחת מידע מאז 2013 (Ji Young, Jong In, & Kyoung Gon, 2019). על פי מדריך הצבא האמריקני ליכולות הצבאיות של קוריאה הצפונית, שפורסם ביולי 2020, ביחידה 121 מועסקים יותר מ-6,000 אנשים, ורבים מהם פועלים ממדינות אחרות כמו בלארוס, סין, הודו, מלזיה ורוסיה. ליחידה 121 ארבע יחידות משנה:

- מערך התקיפה Andarial, שבו מועסקים כ-1600 איש; תפקידו הוא איסוף מודיעין ממערכות מחשב ומיפוי רשתות לקראת תקיפה.
  - מערך Bluenoroff, שבו מועסקים כ-1700 איש; תפקידו הוא לבצע פשעי סייבר להשגת כסף.
  - מערך לזרוס, שמספר המועסקים בו אינו ידוע; תפקידו הוא לזרות בלבול ועיוורון אצל היריב באמצעות תקיפת חולשות ברשתות והטמנת "כפתורים אדומים" להשמדת מערכות בתזמון מאוחר.
  - חטיבת לוחמה אלקטרונית.
- נוסף על כך, על פי המדריך הצבאי, מאז שנת 2009 מכשירה המכללה הצבאית ללוחמה אלקטרונית בפיוניגיאנג, מכללת מירים (Mirim College), כ-100 האקרים מדי שנה עבור צבא קוריאה הצפונית (Department of the Army, 2020).

א. יחידה 180 – מסגרת סייבר צבאית שנועדה לפעול בצורה חשאית נגד יריבים בין-לאומיים. על פי ההערכות, קוריאה הצפונית משתמשת ביחידה זו כדי להשיג מטבע זר, והיחידה נחשדת במעורבות נרחבת בפריצות לבנקים וגנבת כסף; בין היתר נחשדת היחידה כקשורה למערך התקיפה המכונה "לזרוס" (Lazarus), אשר תקף את מסלוקת הבנקים הבינלאומית SWIFT (Ji Young, Jong In & Kyoung Gon, 2019). היחידה פועלת באופן מבוזר – אנשיה פועלים מחוץ למדינה, במקומות שבהם קיימת תקשורת מהירה, ולעיתים משמשים בתפקידי דים בחברות טכנולוגיות מידע או היי-טק בדרום מזרח אסיה ואף במזרח אירופה. במקרים מסוימים פועלת היחידה בכיסוי של הלשכה המרכזית לסטטיסטיקה (CBS – Central Bureau of Statistics).

ב. מערך התקיפה לזרוס (מכונה גם APT38 ו-<sup>3</sup>Hidden Cobra) – מערך זה פועל מאז 2009 לפחות, ויכולותיו טובות מאוד. ככל הידוע, המערך מפעיל שני מערכי משנה: BlueNorOff – תקיפת בנקים ומערכות פיננסיות נוספות כדי לגנוב מהם כסף עבור המדינה; Anderiel – תקיפת ארגונים אחרים במזרח הרחוק, בארצות הברית ובמזרח התיכון. למערך לזרוס מיוחסת תקיפת אולפני סוני (Baezner, 2018; Pearson & Park, 2017), ובעבר הוא השתמש בחברת קש בשם JMT trading לתקיפות (Barth, 2019).

בקוריאה הצפונית פועלים גופי סייבר נוספים השייכים ככל הנראה ל-RGB, אולם מקומם במדרג בתוך הסוכנות אינו ברור:

א. APT37 – המערך מוכר מאז 2012 ופועל מול גורמים במזרח הרחוק ובמזרח התיכון. הוא מתמקד בתעשיות שונות, ובכללן כימיקלים, חלל, רכב, בריאות ואלקטרוניקה (FireEye, 2018), וידוע כי הוא מפעיל חולשות "יום ס".

ב. Temp.Hermitn, Temptick, Stardust Chollima, Kimsuki – מערכים המבצעים פעולות ריגול ותוקפים בנקים ומערכות פיננסיות נוספות כדי לגנוב כסף עבור המדינה (Nakamura, 2013, Tarakanov, & Kim).

על פי פרסומיו של סנודן, ארצות הברית וקוריאה הדרומית הצליחו לחדור למערכות RGB כמה פעמים (Sanger, Kirkpatrick, & Perlroth, 2017).

אגף ה"תקשוב" (CMA – Command Automation Bureau)

האגף ה"תקשוב" הוא אחד מאגפי GSD, ואחראי לתקשורת הצבאית ובמסגרת זו גם לפעילות המשיקה לעולם הסייבר; ייתכן כי יחידותיו פועלות גם עבור RGB. קיים מידע על חלק מן היחידות באגף זה:

- א. יחידה 31 – עוסקת בין השאר בפיתוח נזקקות;
- ב. יחידה 32 – אחראית לפיתוח תוכנה לשימושים צבאיים;
- ג. יחידה 56 – אחראית לפיתוח תוכנות פיקוד ושליטה (Ji Young, Jong In & Kyoung Gon, 2019).

מרכז המחשבים של קוריאה הצפונית (KCC – Korea Computer Center)

מרכז המחשבים הוא מרכז המחקר הממשלתי של קוריאה הצפונית ומרכז מוביל בתחום טכנולוגיות המידע. ל-KCC יש 11 מרכזי פיתוח וייצור טכנולוגיות מידע אזוריים וסניפים במדינות נוספות, בהן סין, סוריה, גרמניה ואיחוד האמירויות הערביות. ידוע כי במרכז עוסקים במחקר לינוקס ובפיתוח מערכת ההפעלה הלאומית "כוכב אדום". ל-KCC פרויקטים נוספים, וחלקם משמשים אף את יחידות התקיפה בסייבר למטרותיהן: רשת האינטראנט הלאומית; מנוע חיפוש בבעלות המרכז; מעבד תמלילים; משחק מחשב (Jang-Gi) המאפשר לעקוב אחר המשתמשים ולגנוב את פרטיהם ואת כספם; תוכנית לימודים בנושא תזונה; עורך שיטת קלט בשפה הקוריאנית; תרגומן מאנגלית לקוריאנית ומקוריאנית לאנגלית; תוכנת זיהוי קול; מערכת לשיחות ועידה בווידיאו; מערכת למידה מרחוק.

נוסף על מחקר ופיתוח, ה-KCC אחראי לניטור אתרי אינטרנט של ממשלות זרות וגופים עסקיים זרים, ומנהל מבצעים טכנולוגיים לפגיעה במערכות טכנולוגיה זרות. במסגרת זו מעורב ה-KCC בפעולות סייבר ומשמש למעשה מרכז הפיקוד של פעולות אלו.

3 לפי חברת האבטחה McAfee, לזרוס הוא למעשה אחד מארבעה מערכי תקיפה (Lazarus, Kimsuky, KONNI, APT37) אשר אוגדו יחד בכינוי Hidden Cobra (McAfee Labs, 2020).

4 חולשות שאינן מוכרות לגורמי הגנה עד לרגע שבו מתבצעת באמצעותן פגיעת סייבר.



גורמי סייבר הפועלים במסגרת גופי ממשל נוספים ויחידות הכפופות למרכז המפלגה

למפלגת הפועלים של קוריאה הצפונית כפופות כמה יחידות העוסקות בסייבר. הוועדה המרכזית של המפלגה מפקחת על יחידה 35 (יחידת החקירות המרכזית של המפלגה), אשר אחראית להכשרתם של לוחמי סייבר ולחינוכם הטכנולוגי. הלשכה המרכזית לסטטיסטיקה (CBS) אחראית ללוחמת מידע והשפעה – לוחמה פסיכולוגית בסייבר וריגול בארגוני פנים; היא מפקחת על יחידה 204, אשר אחראית למחקר טכנולוגי וכן לתכנון ולביצוע פעולות לוחמה פסיכולוגית בסייבר. כאמור, יחידה 180 פועלת גם היא לעיתים בכיסוי של הלשכה המרכזית לסטטיסטיקה (Pearson & Park, 2017). גם המחלקה לפעולות פסיכולוגיות של ועדת ההגנה הלאומית עוסקת בלוחמה פסיכולוגית בסייבר.

לשכה 225 אחראית להכשרת סוכנים, להחדרת סוכנים לקוריאה הדרומית ולפעילות מחתרית במדינה. פעילותה היא בעיקר בתחום המודיעין הקלאסי, אך היא משמשת גם להחדרת כלים לתקיפות סייבר בסיוע בני אדם (HUGINT) (Park, 2016).

מחלקת החזית המאוחדת (UFD – United Front Department) עוסקת במבצעים גלויים לעידוד אהדה בקוריאה הדרומית לקוריאה הצפונית.

גופי ממשלה נוספים אשר עוסקים במודיעין, בתשתית טכנולוגית ובפיתוח הם משרד תעשיית האלקטרוניקה, משרד הדואר והתקשורת ומרכז המידע המדעי והטכנולוגי (CSTIA – Central Scientific and Technological Information Agency) – גוף אשר אוסף נתונים בנושאי מדע וטכנולוגיה מתקדמים, מנתח ומעבד אותם, והוא כנראה מכון המחקר המדעי הגדול ביותר של קוריאה הצפונית.

#### אירועי תקיפה נבחרים במרחב הסייבר המיוחסים לגורמים מקוריאה הצפונית

בעשורים האחרונים ביצעו גורמים מקוריאה הצפונית תקיפות רבות במרחב הסייבר. כלל הידע בעניין מבנה המשטר ויכולות התקשורת האלקטרונית במדינה, ובעיקר רוחב הפס וחוסר היכולת של גורמים שאינם קשורים לממשל לגשת לאינטרנט, מצמצמים עד מאוד את הסבירות לקיומן של קבוצות האקרים עצמאיות. בשל כך, כלל התקיפות המיוחסות לקוריאה הצפונית מזוהות עם גורמי המשטר, וככל הנראה בוצעו מטעמו.

במסגרת פעילות זו, שבחלקה הגדול נועדה להגדיל את הכנסות המדינה ולסייע בתקצוב הפרויקטים החשאיים שלה (בפרט פרויקטי הגרעין והטילים), נעשו פעולות לגנבת כספים מבנקים, מארגונים, מחברות ומאנשים פרטיים, ובוצעו תקיפות לשם קבלת כופר. כמו כן נעשו פעולות לגנבת מידע רלוונטי מתעשיות ביטחוניות בעולם המערבי – שמטרתן להתגבר על חסמים בפרויקטים חשאיים של קוריאה הצפונית ולקצר את תהליכייהם, ופעולות לגנבת מידע מחברות אבטחת סייבר, כדי ללמוד כיצד להתגבר על מערכי ההגנה ולשפר את פעילות גורמי הסייבר של המדינה.

להלן יפורטו כמה אירועי תקיפה בולטים במיוחד במרחב הסייבר אשר מיוחסים לקוריאה הצפונית; חלק מהתקיפות הצליחו מאוד וחלקן פחות, אולם הן מצביעות על תעוזתם של התוקפים ועל האידאולוגיה שביסוד פעולתם:

• בינואר 2003 שיתקה התקפה אלקטרונית קשה חלקים מרשת האינטרנט במזרח אסיה והאטה את הגלישה ברחבי העולם; כ-200,000 מערכות ברחבי העולם נפגעו. ההתקפה

בוצעה באמצעות הנוזקה "Slammer" (המכונה גם SQ hell ו-Sapphire). יש חוקרי אבט"ח המשייכים תקיפה זו לקוריאה הצפונית, אולם אין בידינו מקורות התומכים בטענה זו. בשנת 2004 חדרו גורמי תקיפה מקוריאה הצפונית ל-33 רשתות תקשורת צבאיות של קוריאה הדרומית (Fox-Brewster, 2014).

• ביוני 2006 תקפה קוריאה הצפונית יעדים של מחלקת המדינה של ארצות הברית בעת המשא ומתן על הבדיקות שיערכו לטילים הגרעיניים של קוריאה הצפונית. חודש לאחר מכן פרצה יחידה 121 ליעדים בקוריאה הדרומית ובארצות הברית (Fox-Brewster, 2014).

• בשנת 2011 עצרה משטרת קוריאה הדרומית חמישה אנשים אשר ניסו לגנוב כסף דרך משחקים מקוונים, ובהם אזרח סין, באשמת פעילות עבור גורמי תקיפה מקוריאה הצפונית המשתייכים למרכז המחשבים (KCC).

• בשנת 2013 הושבתו כ-30 אלף מחשבים של בנקים בקוריאה הדרומית (Sang-Hun, 2013). באותה שנה דווח בקוריאה הדרומית כי קוריאה הצפונית משתמשת במשחקי מחשב כדי להחדיר נזקות למערכות ולפגוע בהן – דרך הורדת משחק הותקן בכ-100,000 מחשבים Botnet (מערך תוכנות) והופעלה מתקפת DDoS<sup>5</sup> נגד מערכות נמל התעופה הבין-לאומי של סאול.

• במרץ 2013, בזמן שכוחות צבאיים מקוריאה הדרומית ומארצות הברית ניהלו תרגיל משותף, חוו בנקים וגופי שידור בקוריאה הדרומית שיבושים ברשתות התקשורת שלהם. בתקיפה זו, שיצאה מכתובת IP בסין, הצליחה נוזקה בשם DarkSeoul (שכבר זוהתה בעבר) לחמוק מתוכנת אבטחה של קוריאה הדרומית, להפוך את המחשבים שהותקפו לבלתי שמישים ולשבש את התקשורת.

• בינואר 2014 נפרצו שרתי סוכנות האשראי של קוריאה הדרומית ונגנבו פרטיהם של כ-20 מיליון לקוחות; יועץ חיצוני לסוכנות ניצל לרעה גישה למידע כדי לסייע לתוקפים. באותה השנה הותקפו גם מערכות הפעלה של כור גרעיני בקוריאה הדרומית, דרך שרתים סיניים (Credit card details on 20 million South Koreans stolen, 2014; Park & Cho, 2015).

• ביוני 2016 נפרצו יותר מ-140,000 מחשבים ב-160 סוכנויות ממשלתיות וחברות מקוריאה הדרומית; במחשבים שנפרצו נשתל קוד, כחלק ממתקפת APT<sup>6</sup> (Pearson & Park, 2017). באותה שנה תקף מערך BlueNorOff עשרות בנקים באירופה בניסיון לגנוב כסף.

• בשנת 2017 ניסו האקרים מקוריאה הצפונית לתקוף כמה בנקים בפולין. אף על פי שהתקפות החוזרות ונשנות לא צלחו, שיטות התקיפה היו מתוחכמות יותר ממה שציפו לו מומחי אבטחה רבים. האקרים אלו תקפו מוסדות נוספים, ובהם ארגונים פיננסיים בארצות הברית, הבנק העולמי ובנקים ברוסיה ובאורוגוויי.

• בשנת 2019 הותקפו גורמי תעשייה ביטחונית ישראלית (Yaron, 2019).

• ביוני 2020 הותקפו בשורת תקיפות סייבר חברות ביטחוניות בתחום התעופה והחלל במדינות שונות במערב, בניסיון להשיג מידע מודיעיני רגיש (ESET, 2020).

• באוגוסט 2020 פורסם כי מערך תקיפה מדינית – בסבירות גבוהה "לזרוס" – פנה בהצעות עבודה מפתות לעובדי תעשיות ביטחוניות בישראל באמצעות הרשת החברתית LinkedIn, כדי לחדור לרשתות המחשב שלהם ולתקוף אותן (הטוני, 2020).

5 תקיפה מבוצרת של מערכת מחשב או רשת באמצעות שימוש במערכות רבות כדי להציאה מכלל פעולה.

6 תקיפה מתמשכת וממוקדת שמבצעים ארגונים חזקים או מדינות באמצעות מגוון כלי תקיפה וטכניקות חדירה.

## מקרי מבחן

להלן יוצגו כמה אירועי תקיפה במרחב הסייבר, אשר מייצגים את "תרבות" תקיפות הסייבר בקוריאה הצפונית. חשיבותם של האירועים נובעת בעיקר מן הנזק הרחב שגרמו לו ומן הפרסום הרב שזכו לו.

### תקיפת חברת סוני (Sony) בשנת 2014

בנובמבר 2014 הותקפו שרתי חברת סוני האמריקנית; התקיפה נועדה למנוע את יציאתו לאקרנים של הסרט "הריאיון", שמתאר שחקני קולנוע המגויסים לרצוח את מנהיג קוריאה הצפונית (Siboni & Siman-Tov, 2014). התוקפים לא השיגו את מטרם.

לפני התקיפה בפועל, בסוף נובמבר, קיבלו אנשי חברת סוני דרישת כופר אנונימית להעברת כספים בתמורה לכך שמחשבי החברה לא ייפגעו. כמה ימים לאחר מכן הותקפה רשת מחשבים של סוני – מידע רב שאוחסן ביחידות שונות נמחק, ולחלק מן המחשבים הוחדר מסר של גוף שהציג עצמו בשם "ארגון שומרי השלום" והזדהה כמי שביצע את התקיפה. לאחר מכן התרחשו כמה אירועים שנועדו להפעיל לחץ חברתי וכלכלי על חברת סוני לשנות את תוכניותיה בנוגע לסרט: מידע סודי השייך לחברה פורסם באתרים לשיתוף קבצים במשך כמה שבועות, וחלק מעובדי החברה קיבלו איומים אנונימיים כי אם לא יגנו את פעולותיה של החברה ייפגעו פגיעה פיזית.

תקיפת סוני שונה מתקיפות אחרות משום שהיה בה אלמנט הרסני: עד אותו מקרה תקיפות סייבר של קוריאה הצפונית הוגדרו כגורמות שיבוש בלבד, ללא נזק פיזי (למשל באמצעות השחתת אתרים או התקפות DDoS), ואילו בתקיפה של סוני רוב תחנות העבודה שנפגעו ניזקו באופן קשה ונדרש להחליפן.

אף שבקרב קהילת המודיעין האמריקנית נשמעו הטענות כי יש בידי ארצות הברית הוכחה למעורבות קוריאה הצפונית בתקיפה של סוני, מומחי אבטחת מידע שונים פקפקו ביכולתה של קוריאה הצפונית לבצע התקפות כה הרסניות ותהו אם בנוזקה המעורבת בתקיפה נמצאו סימנים הקושרים אותה לתקיפה (Bradner, 2014).

ב-19 בדצמבר 2014 כינה נשיא ארצות הברית ברק אובמה את התקיפה "cyber vandalism", והתחייב להגיב לה במקום, בזמן ובדרך שארצות הברית תמצא לנכון. מזכיר המדינה כינה את התקיפה "האקט הבוטה ביותר של טרור ומלחמה", ואיים בצעדי תגובה קשים (Bradner, 2014). ב-20 בדצמבר דיווחו מומחי סייבר וגופי חדשות שהרשת בקוריאה הצפונית שמעניקה גישה לרשת האינטרנט העולמית הושבתה לזמן משוער של עשר שעות. הם לא ידעו לומר אם היה זה צעד מניעתי של המדינה עצמה או שמדובר בתקיפה שמקורה חיצוני. גורמים רשמיים בארצות הברית לא התייחסו לאירוע, אך ציינו שחלק ממרכיבי "התגובה הראויה" יהיו גלויים ואילו אחרים לא (Bradner, 2014).

דבריו של עוזר מנהל יחידת הסייבר ב-FBI ג'וזף דמארסט (Joseph Demarest) בשימוע שנערך בסנאט בנושא מלמדים עד כמה משוכללת הייתה התקיפה: "הנוזקה שבה נעשה שימוש כדי לפרוץ לסוני הייתה מצליחה לעבור דרך כ-90% ממערכות ההגנה הקיימות בתעשייה האזרחית ובמערכות הממשל" (Elkind, 2015). גם ראש המודיעין הלאומי האמריקני (Director of National

Intelligence) ג'יימס קלפר (James Clapper) סבר כי מבין תקיפות הסייבר שנועדו לפגוע באינטרסים של ארצות הברית, הייתה זו החמורה ביותר (Flitter, E. & Hosenball, 2015). מהתבטאויות אלה אפשר ללמוד על כך שמומחי המערב לא העריכו נכון את יכולות הסייבר של קוריאה הצפונית; אף שהיא נתונה בבידוד מדיני ושהנגישות לאינטרנט מוגבלת בה מאוד, איששה התקיפה נגד סוני את ההנחה שיש ברשות קוריאה הצפונית יכולות מתקדמות.

### תקיפת בנקים בבנגלדש בשנת 2016

בפברואר 2016 נגנב סכום של כ-81 מיליון דולר בסדרת מתקפות סייבר על בנקים בבנגלדש ובדרום-מזרח אסיה. חוקרים קישרו את המתקפות לקוריאה הצפונית, וצינו כי נמצא דמיון בין הקוד שנעשה בו שימוש במקרה זה לקוד שנעשה בו שימוש בתקיפות קודמות מצד קוריאה הצפונית. בתקיפה זו השתמשו ההאקרים במערכת הסליקה והעברת הכספים הנפוצה של SWIFT כדי להעביר כספים מהבנק המרכזי של בנגלדש לחשבונות בפיליפינים, באמצעות נזקה שהוחדרה למסוף SWIFT בבנק המרכזי בבנגלדש. הרשת בבנגלדש הייתה ככל הנראה רגישה במיוחד, מאחר שלא הייתה בה חומת אש (firewall) להגנה מפני חדירות. התוקפים העבירו מסרים כוזבים בין בנקים בניו יורק לבנקים בבנגלדש כדי לגרום להעברת כספים בין הבנקים, ושינו את המסמכים הנלווים לביצוע ההעברות כדי לטשטש את עקבותיהם (Hammer, 2018). לכתחילה ביקשו ההאקרים לקבל מיליארד דולר מבנקים שונים, אך מכיוון שהבנק המרכזי בארצות הברית דחה את רוב הבקשות – הם לא הצליחו לגנוב את מלוא הסכום.

ב-21 במרץ 2017 הציג סגן מנהל ה-NSA ריצ'רד לדג'ט (Richard Ledgett) מחקר שהראה קשר בין תקיפה זו לתקיפה של סוני, וציין כי אם יוכח שקוריאה הצפונית אחראית לתקיפת הבנק – מדובר ביכולת חדשה ומדאיגה שלה. יש חוקרים הסבורים כי מתווכים סינים סייעו לקוריאה הצפונית בביצוע הגנבה, ואילו אחרים האשימו האקרים סינים בביצוע התקיפה.

נוסף על הבנק בבנגלדש תקפו ההאקרים בנקים נוספים שהשתמשו ב-SWIFT; על פי דו"ח של חברת אבטחת המידע קספרסקי, קוריאה הצפונית אחראית למתקפות דומות על בנקים במדינות נוספות. חוקרי האבטחה סבורים שאותם האקרים אחראים גם לשיטת תקיפה נוספת של בנקים, המכונה "watering hole" – שיטה שבה התוקפים מגיעים לאתרים שהתנועה בהם רבה ומנסים לכוון את התנועה לאתר המכיל נוזקה. בסופו של דבר, כאמור, לא הצליחו התוקפים לממש את יעדם העיקרי – גנבת כמיליארד דולר (GReAT, 2017).

### המתקפה העולמית של כופרת WannaCry בשנת 2017

ב-12 במאי 2017 דיווחו ארגונים מרחבי העולם על מתקפת כופרה אשר משפיעה על רשתות המחשבים שלהם ומגבילה את גישת המשתמשים למחשביהם עד שישלמו את הכופר שהוצג. הכופרה פגעה ביותר מ-300 אלף משתמשים מ-150 מדינות; היא הופצה בהתקפות "דיוג" (phishing) אך התפשטה מהר יותר מכופרה רגילה משום שניצלה חולשות אבטחה כדי לנוע מהר יותר בין מחשבים לא מוגנים (Pearson & Park, 2017).

## סיכום

על אף המאפיינים הייחודיים הנובעים ממצבה הגאופוליטי של קוריאה הצפונית, היא הצליחה לפתח יכולות וכלים מתקדמים ומפותחים ביותר במרחב הסייבר, כמעט כשל מעצמה. יכולות וכלים מרשימים אלה מאפשרים לה לתקוף מדינות רבות באסיה ובמערב בתקיפות סייבר רחבות היקף. ככל הידוע, קוריאה הצפונית היא המדינה היחידה שמפעילה את גורמי התקיפה שלה למטרות גנת כסף ולביצוע פשעים. תקיפות הסייבר מאפשרות למדינה להתחמק מן הסנקציות הבין-לאומיות המוטלות עליה, ולהשיג רווח כלכלי שיאפשר לה להקצות משאבים לכרויקטי פיתוח אמצעי הלחימה הסודיים של המדינה ולמימוש שאיכותיה בתחום הגרעין.

ייחודיותם של כלי התקיפה של המדינה היא גם נקודת החולשה שלה; לעיתים, מנגנוני החוסן של קוריאה הצפונית מהונדסים באופן חריג יתר על המידה, המאפשר את ייחוסם למדינה. חשיפתם של כלי התקיפה עלולה לגרום לפגיעה רוחבית למדינה, וזוהי חולשה שאפשר לנצל כדי להתמודד עם תקיפות מצידה.

מנהיגה של המדינה הטוטליטרית הסגורה פועל באופן המקשה מאוד על ניסיון לנבא את מהלכיו. עם זאת, המשכיות המצב הגאופוליטי והצלחותיהם של גורמי הסייבר מובילים אותנו להעריך כי פעילות ההתקפית של קוריאה הצפונית במרחב זה תימשך ואף תתגבר, וכי מנהיג המדינה עשוי להחליט על פעילות נגד יעדים ישראליים מבלי שיהיה על כך מידע מקדים. אומנם ישראל עדיין אינה נמצאת במוקד העניין של קוריאה הצפונית, אולם זו כבר הוציאה לפועל מבצעי תקיפה במרחב הסייבר נגד גורמים ישראליים; כמו כן, היא מקיימת קשרים הדוקים עם אויבי ישראל ועלולה לסייע להם גם במרחב זה.

עוד ראוי להביא בחשבון כי גורמי הסייבר של קוריאה הצפונית יעסקו באיסוף מודיעין מחברות תעשייה ביטחונית ומפרויקטים ישראליים בשיתוף ארצות הברית שעשויה להיות להם זיקה לדרום-מזרח אסיה (דוגמת מכירת טכנולוגיות לקוריאה הדרומית, לסינגפור, ליפן ולהודו).

תמיכתה של המדינה באויבי ישראל והתפיסות המנחות את מנהיגה מצדיקים, לטעמנו, לדון באפשרות להפעיל יכולות איסוף כלפי גורמים בקוריאה הצפונית אשר משתמשים במרחב הסייבר כדי לבצע פעולות נגד יעדים ישראליים ובין-לאומיים.

לאור כל האמור לעיל ראוי לדעתנו כי קובעי המדיניות בישראל ידונו באפשרויות להרחבת בסיס הידע על פעילות גורמי הסייבר של קוריאה הצפונית.

המתקפה פגעה פגיעה קשה מאוד במערכת הבריאות הבריטית – מידע רפואי של בתי חולים ציבוריים וקליניקות רפואיות הוצפן ולמעשה הושמד; מצב זה גרם לדחיית תורים וטיפולים רפואיים וכפועל יוצא – לפגיעה בחיי אדם. פגיעה קשה נגרמה גם למערך הרכבות הגרמני, לחברת השליחויות האמריקנית Fedex, לבנק BBVA הספרדי, למפעילת התקשורת הספרדית Telefónica, לכמה אוניברסיטאות ולכמה סניפים של פירמת רואי החשבון KPMG. הפגיעות הקשות ביותר נגרמו למשתמשים מרוסיה, מאוקראינה, מהודו ומטייוואן. כלי התקיפה שבו נעשה שימוש היה קוד המייצג חולשה במערכת, חלק מכלי תקיפה שנגנב מה-NSA.

חודשים לפני המתקפה, בקיץ 2016, חשפה קבוצה הידועה בשם The Shadow Brokers כי בידיהם מגוון אמצעי תקיפת סייבר שנגנבו מה-NSA, וכי הם ניצלו חולשה באבטחת מערכת Windows הידועה בשם EternalBlue. במרץ 2017 תיקנה חברת מיקרוסופט את הבעיות שנוצלו בכלים אלה. לימים התברר כי אחד מן העדכונים לתוכנה בעקבות התיקון הגן עליה מפני התפשטותה של כופרת WannaCry, וכי רק מערכות שלא התקינו את העדכון נפגעו מן הכופרה.

קוריאה הצפונית חשודה בכך שהיא יצרה את הכופרה; מומחים העריכו שהיא נוצרה מייד לאחר הפרסום של The Shadow Brokers. על פי דיווחי חדשות ה-NSA פרסמה מסמך פנימי שקשר את הכופרה ל-RGB – הערכת הסוכנות התבססה על כתובות IP שנמצאות בסין ואשר ידוע שהן משמשות את ה-RGB, ולכן יוחסה יצירת הכופרה לקוריאה הצפונית במידת ביטחון בינונית (Pearson & Park, 2017).

ההאקרים שהפיצו את הכופרה הם ככל הנראה מקבוצת לזרוס, שהייתה אחראית גם לתקיפה שתוארה לעיל על SWIFT בפברואר 2016. בשני המקרים, התקיפות בוצעו ככל הנראה כדי לנסות לגייס כספים עבור המשטר בקוריאה הצפונית. אולם יש מומחים הסבורים כי הצגת דרישת התשלום במטבע דיגיטלי וכמה פגמים שנמצאו בכופרה מעידים על כך שהתוקפים היו מעוניינים להשיג רווח כלכלי אישי.



[fee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true](#)

Mercado, S. C. (2004). Hermit surfers of Pyongyang: North Korea and the Internet. *CIA Studies in Intelligence*, 48(1). <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no1/article04.html>

Nakamura, Y., & Kim, S. (2017, September 11). North Korea is dodging sanctions with a secret Bitcoin stash. *Bloomberg Businessweek*. <https://www.bloomberg.com/news/articles/2017-09-11/north-korea-hackers-step-up-bitcoin-attacks-amid-rising-tensions>

Nichols, M. (2019, August 5). North Korea took \$2 billion in cyberattacks to fund weapons program: U.N. report. *Reuters*. <https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UViZX>

North Korea's 'paranoid' computer operating system revealed. (2015, December 27). *The Guardian*. <https://www.theguardian.com/world/2015/dec/27/north-korea-computer-operating-system-revealed-by-researchers>

Office of the Secretary of Defense (2015). Military and security developments involving the democratic people's republic of Korea – A Report to Congress. [https://dod.defense.gov/Portals/1/Documents/pubs/Military\\_and\\_Security\\_Developments\\_Involving\\_the\\_Democratic\\_Peoples\\_Republic\\_of\\_Korea\\_2015.PDF](https://dod.defense.gov/Portals/1/Documents/pubs/Military_and_Security_Developments_Involving_the_Democratic_Peoples_Republic_of_Korea_2015.PDF)

Park, D. (2016, June 28). North Korea cyber attacks: A new asymmetrical military strategy. *The Henry M. Jackson School of International Studies*. <https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/>

Park & Cho, (2015, March 17). South Korea blames North Korea for December hack on nuclear operator. *Reuters*. <https://www.reuters.com/article/us-nuclear-southkorea-northkorea/south-korea-blames-north-korea-for-december-hack-on-nuclear-operator-idUSKBN0MD0GR20150317>

Pearson, J., & Park, J. (2017, May 21). Exclusive: North Korea's unit 180, the cyber warfare cell that worries the west. *Reuters*. <https://ca.reuters.com/article/newsOne/idCAKCN18H020-OCATP>

Person, J. (2014). Origins of North Korea's Juche: Colonialism, war, and development. *Pacific Affairs*, 87(3), 621–624.

from [https://www.globalfirepower.com/country-military-strength-detail.asp?country\\_id=north-korea](https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=north-korea)

GReAT (2017, April 3). Lazarus under the hood. *SecureList*. <https://securelist.com/lazarus-under-the-hood/77908/>

Hammer, J. (2018, May 3). The baby-formula crime ring. *The New York Times – The Money Issue*. <https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html?mtrref=undefined&gwh=A827CC56B2EAB65EAE62E1DEBCA83528&qwt=pay&assetType=PAYWALL>

Jaewon, K. (2017). A cybersecurity defector warns of North Korea's 'hacker army'. *Nikkei Asia Review*. <https://asia.nikkei.com/Politics/A-cybersecurity-defector-warns-of-North-Korea-s-hacker-army>

Ji Young, K., Jong In, L., & Kyoung Gon, K. (2019). The all-purpose sword: North Korea's cyber operations and strategies. In T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, & G. Visky (Eds.), 11<sup>th</sup> International conference on cyber conflict: Silent Battle International Conference on Cyber Conflict: Silent battle (pp. 143–162). Talin, Estonia: NATO CCD COE Publications

Jun, J., LaFoy, S., & Sohn, E. (2016). North Korea's cyber operations: Strategy and responses. *CSIS*. [https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy\\_files/files/publication/151216\\_Cha\\_NorthKoreasCyberOperations\\_Web.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf)

Kim, S. H. (2015). The survival of North Korea: A case for rethinking the US-North Korea nuclear standoff. *North Korean Review*, 11(1), 101–13.

Kovacich, G. L., & Jones, A. (2016). *Global information warfare: The new digital battlefield* (2nd ed.). Boca Raton, FL: CRC Press.

Lankov, A. (2017, May 1). On the great leader's secret service: North Korea's intelligence agencies. *NK News*. <https://web.archive.org/web/20180731080639/https://www.nknews.org/2017/05/on-the-great-leaders-secret-service-north-koreas-intelligence-agencies/>

Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, 1(1), 53–67.

McAfee Labs. (2020, July 29). Operation (노스 스타) North Star – A job offer that's too good to be true? McAfee. <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/>

- Poznansky, M. (2020). Revisiting plausible deniability. *Journal of Strategic Studies*. <https://doi.org/10.1080/01402390.2020.1734570>
- Ramani, S. (2018, February 27). North Korea's Syrian connection. *The Diplomat*. <https://thediplomat.com/2018/02/north-koreas-syrian-connection/>
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), 4–37.
- Sanger, D. E., Kirkpatrick, D. D., & Perloth, N. (2017, October 15). The world once laughed at North Korean cyberpower. No more. *The New York Times*. <https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html>
- Sang-Hun, C. (2013, March 20). Computer networks in South Korea are paralyzed in cyberattacks. *The New York Times*. <https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html>
- Siboni, G., & Siman-Tov, D. (2014, December 23). Cyberspace extortion: North Korea versus the united states. *INSS Insight*. <https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/SystemFiles/No.%20646%20-%20Gabi%20and%20Dudi%20for%20web.pdf>
- Socialist constitution of the Democratic People's Republic of Korea (2017). <http://www.korean-books.com/kp/KBMbooks/en/book/politics/00000450.pdf#page=29>
- Tarakanov, D. (2013, September 11). The "Kimsuky" operation: A North Korean APT? *SecureList*. <https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915>
- Terry, D. P., & Wood, A. F. (2015). Presenting Juche: Audiencing North Korea's 2012 Arirang mass games. *Text and Performance Quarterly*, 35(2–3), 177–201.
- Williams, M. (2019, July 22). North Korea's koryolink: Built for surveillance and control. *38 North*. <https://www.38north.org/2019/07/mwilliams072219/>
- Yaron, O. (2019, Mar 26). North Korean hackers cited in rare attack in Israel. *Haaretz*. <https://www.haaretz.com/israel-news/business/.premium-north-korean-hackers-cited-in-rare-attack-in-israel-1.7059457>

קוראיה הצפונית היא מדינה שמצבה הגאופוליטי גוזר עליה מאפיינים ייחודיים – היא מבודדת ומנותקת ממרבית מדינות העולם ונתונה לסנקציות באופן תמידי. למרות זאת היא הצליחה לפתח יכולות תקיפה בלתי מבטולות במרחב הסייבר, המאפשרות לה לתקוף מדינות רבות באסיה ובמערב בתקיפות סייבר רחבות היקף. פעולותיה נשענות על אידאולוגיה קשוחה, כמו גם על הסתגרות ובדלנות.

ככל הידוע, קוראיה הצפונית היא המדינה היחידה אשר משתמשת בגורמי התקיפה בסייבר גם לפשעים – גנבה ופעילויות פליליות אחרות – שנועדו להעשיר את קופת המדינה. הרווח מתקיפות במרחב הסייבר מאפשר למדינה להקצות משאבים לפרויקטים לפיתוח אמצעי הלחימה הסודיים שלה, ואגב כך להתחמק מהסנקציות הבינלאומיות המוטלות עליה. פעילותם של גורמי הסייבר של קוראיה הצפונית נועדה לסייע למדינה לממש את שאיפותיה בתחום הגרעין, כדי להתגונן מפני אימום מבית ומחוץ ולצמצם את בידודה משאר מדינות העולם.

סקירה זו מציגה את בסיס הידע הגלוי העדכני על גורמי הסייבר של קוראיה הצפונית ופעילותה במרחב הסייבר על פי פרסומים מן העשור האחרון בעיקר. אף שקוראיה הצפונית אינה מוגדרת באופן רשמי כמדינת אויב, היא נמנית עם יריביה של ישראל, ואף ניסתה לתקוף עובדי תעשיות ביטחוניות ישראליות. מטרתה של סקירה זו היא לזרות אור על יכולות הפעולה הערכניות של קוראיה הצפונית במרחב הסייבר ולהצביע על האיום הפוטנציאלי למדינת ישראל הטמון ביכולות אלו.

**ד"ר הראל מנשרי** הוא ראש תחום סייבר במכון הטכנולוגי חולון (HIT), מרצה בנושא סייבר במחלקה למדע המידע מידע באוניברסיטת בר אילן ועמית מחקר במכון לחקר הטרור במרכז הבינתחומי בהרצליה. בעל עבר של כ-36 שנים במערכת הביטחון.

**גיל ברעם** היא מנהלת קבוצת המחקר של סדנת יובל למדע, טכנולוגיה וביטחון ועמיתת מחקר במרכז הסייבר ע"ש בלווטניק.

### סדנת יובל נאמן למדע, טכנולוגיה וביטחון

הוקמה בשנת 2002 על ידי פרופסור אלוף (במיל.) יצחק בן ישראל, בשייתוף עם בית הספר לממשל ולמדיניות ציבורית על שם הרולד הרטוך והתוכנית ללימודי ביטחון באוניברסיטת תל-אביב, במטרה לעסוק בממשק שבין המדע והטכנולוגיה לביטחון. לשם כך, הסדנה מקיימת פעילות מחקרית ענפה, אשר כוללת מחקרים ופרסום ניירות עמדה בתחום מדיניות הביטחון הלאומי, לצד סדרה שנתית של כנסים וימי עיון המתקיימים באוניברסיטת תל-אביב. מטרת פעילותה של הסדנה היא ליצור דיאלוג פתוח ופורה עם הציבור הרחב המתעניין בתחומי ההתמחות העיקריים של הסדנה - אבטחת סייבר וחלל – ובתחומי עיסוק נוספים: יחסים בינלאומיים ואסטרטגיה, בינה מלאכותית, טילים ונשק מונחה, רובוטיקה, יחסי הגומלין בין החברה לביטחון, אנרגיה גרעינית, ביטחון פנים, מדיניות בניין הכוח, תהליכי קבלת החלטות ועוד.



Blavatnik Interdisciplinary  
Cyber Research Center



אוניברסיטת  
תל אביב  
TEL AVIV  
UNIVERSITY



Yuvael Ne'eman Workshop  
for Science, Technology and Security  
Tel Aviv University