



Atlantic Council

SCOWCROFT CENTER  
FOR STRATEGY AND SECURITY



הסכסוך הערבי-ישראלי

סמינר הנאמנות הירדנית/ישראלית לחזוק השת"פ בענייני הגנה ובטחון

בטחון סייבר

SIMON HANDLER

# הנושא

- פריצה ודליפה של מידע רגיש מצד שחקנים שהם מדינות ולא-מדינות יוצר נזקים צדדיים לבטחון הלאומי. אף על פי שבינה מלאכותית (ב"מ) יכולה לתרום למספר איומי הסייבר, היא יכולה גם לשמש כדי לגלות ולמתן אותם. ישיבה זו תבחן ותשאל איך פתרונות בטחון סייבר מונעי ב"מ יכולים לעזור לשתי המדינות ולתרם ליציבות האזורית.

# ההרצאה של היום

■ להבין פעולות פריצה ודליפה

- סבות, אמצעים, ותוצאות

- דוגמאות בולטות

■ להביט מחוץ לאזור

■ איומים אזוריים במזה"ת

■ לאפיין את תחום הסייבר

■ מסגרת חדשה לאסטרטגיית סייבר

■ יישום האסטרטגיה



# הבנת פעולות פריצה ודליפה

- התכנסות פעולות מידע וסייבר.
- שמוש בסייבר ע"י יריבים (ואפילו בעלי ברית) כדי לזכות בגישה לחמק סודי ורגיש ואז לשתף בו את הצבור
  - מידע
  - כלים
- בעוד המונח 'דליפה' מראה על אמיתיות החומר, פעולות פריצה-ודליפה יכולות לכלול גם מניפולציה.
- ייחוס לא נכון, דגלים מזוייפים, והאפשרות להכחיש.

# סבות, אמצעים ותוצאות

## ■ סבות

- נסיונות מרצון לכוון את דעת הקהל נגד מטרה
- לחשוף את היכולות, הרגישות לפגיעה, וחוסר הוודאות
- פינאנסיות

## ■ אמצעים

- מסרים שקריים
- מסרי חנית שקריים
- דרישות כופר
- התקפות על שרשרות אספקה

## ■ תוצאות, חסרונות וסכונים

- בטחון לאומי, כלכלי, והשלכות חברתיות
- ההשלכות יכולות להיות קשות למדידה אבל יכולות להיות בין השלכות קשות במישטר הפנימי להשלכות במישור החיצוני
- כלי פריצה בתחום הסייבר מספקים כלים ליריבים כדי להשיג ולפרסם חומר סודי, אבל הם מאיימים למשוך תשומת לב למבצע עצמו ולא לשערורייה שבדליפה

# דוגמאות בולטות לפעולות פריצה-ודליפה

- 1929 – האנדרטה לטאנאקה (ממקור לא ידוע)
- 2016 – הוועידה הלאומית של הדמוקרטים (המודיעין הרוסי)
- 2016 – ניירות פאנאמה (ג'והן דו)
- 2017 – הכחול-הנצחי (ברוקרי מללים)
- 2020 – רוחות שמש (לא ידוע כפריצה ודליפה אבל קיים)

# מבט החוזה מהאזור

## ■ שחקנים שהם ארצות

- רוסיה

- צפון קוריאה

- סין

## ■ שחקנים שאינם ארצות

- קבוצות הדורשות כפר-נפש

- פעילי פריצת סייבר

- אנשים פרטיים

# הנוף האזורי

## ■ שחקנים שהם מדינות

- אחוד האמירויות

- ערב הסעודית

- איראן

## ■ שחקנים שאינם מדינות

- חאמאס (קבוצות חפרפרות ועכברושים, כנופיית הסייבר של עזה)

- חזבאללה (ארז הלבנון)



# אפייון תחום הסייבר

■ התחייבויות בלתי סדירות

- המשמשות שחקנים שהם ארצות ולא-ארצות

- תדיר, גישות לא סימטריות

■ סכסוך נמוך-מתח אבל מתמיד

- אזור אפור בין שלום ומלחמה

■ נוף שחלקיו קשורים זה בזה

- אנשים שאינם לוחמים החשופים ללחימה

■ בעיית אבחנה

# מסגרת חדשה לאסטרטגיית סייבר

- הזזת המסגרת מהתקפות קטסטרופיות יחידות
- במקום זאת, למד לקח לסכסוכי סייבר מסכסוכים לא סדירים. אסטרטגיונת של לוחמה בטרור ולוחמה במרידות מספקות לקחים רבי תועלת.
  - מרוץ מודיעיני
  - התפתחות לאורך הזמן
  - היטיב להתחרות

# יישום האסטרטגיה

## ■ צעדים סבילים

- תעדף סכון בלי להסס
- שפר את יכולת ההגנה
- התמקד בכשר ההסתגלות
- התגבר על אי-הצלחות

## ■ צעדים פעילים

- שתוף בזהוי ומידע
- ענישה
- פעולות אכיפת החוק
- הפעל לחץ לשמירה על 'נמלי בית'

Thank you

תודה

شكرا