חלק 1

סייבר

סקירה כללית

איום הסייבר האיראני הוא רק פן אחד של מהפכת המידע האדירה שסחפה את העולם בעשורים האחרונים. כיום הקהילה הבינלאומית יוצרת ביומיים בלבד כמות נתונים השווה בגודלה לכמות שנוצרה מאז ראשית הזמן ועד 2003. בשנת 2019 היה מחשב כמעט במחצית מבתי האב ברחבי העולם. בשנת 2021 כבר היו כ־15 מיליארד טלפונים ניידים, ובשנת 2022 יותר מ־26 מיליארד מכשירים היו מחוברים לאינטרנט.[1] כל מחשב וטלפון מייצגים התקדמות טכנולוגית וחברתית, אך גם משמשים פתח אפשרי לפעילות סייבר זדונית. מהפכת הבינה המלאכותית (AI) היא רק בתחילתה.

בשנים 2005–2019 נגנבו נתונים אישיים של יותר מ־11.5 מיליארד בני אדם ביותר מ־9,000 תקיפות סייבר. בשנת 2012 נאמדה עלות פשיעת הסייבר העולמית ב־8.4 טריליון דולר, והיא צפויה להכפיל את עצמה עד שנת 2025.[2] בתקיפות כופרה הקורבנות נתבעים לשלם כדי לקבל בחזרה גישה למערכות שלהם שהתוקפים הצפינו, והן כיום מובילות את הפשיעה בסייבר ואת תקיפות הסייבר שמניעיהם פוליטיים. לפי הפורום הכלכלי העולמי, פריצות בקנה מידה גדול של אבטחת סייבר הן מחמשת הסיכונים החמורים ביותר שהעולם מתמודד איתם.[3]

1 Statista, "Share of households with a computer at home worldwide from 2005 to 2019"; "Forecast number of mobile devices worldwide from 2020 to 2025 (in billions)"; Josh Howarth, "80+ Amazing IoT Statistics (2023-2030)," exploding topics, March 16, 2023.

2 Mike Isaac and Sheera Frenkel, "Facebook Security Breach Exposes Accounts of 50 Million Users," *New York Times*, September 28, 2018; Brian Fung, "Uber Reaches $148 Million Settlement over its 2016 Data Breach, which Affected 57 Million Globally," *Washington Post*, September 26, 2018; Nicole Perlroth, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," *New York Times*, October 3, 2017; Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth, and Ron Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S." *New York Times*, September 7, 2017; The Economist, "The Big Data Breach Suffered by Equifax Has Alarming Implications," September 16, 2017; Statista, "Estimated Cost of Cybercrime Worldwide 2017-2028."

3 U.S. Department of Homeland Security, "Cybersecurity Strategy," 2018, 2; Shoshana Solomon, "Israeli Entrepreneur Calls for NATO-Style Cybersecurity," *Times of Israel*, January 31, 2018.

לתקיפות סייבר על הצבא עשויות להיות השלכות חמורות במיוחד. הן עלולות להשבית מערכות נשק או לפגוע בדיוק שלהן, לשבש את התקשורת ואף להשפיע על המורל של החיילים ושל החברה האזרחית. לתקיפות סייבר מוצלחות על מטרות חיוניות שאינן צבאיות עשויה להיות השפעה מערכתית על יכולות הלחימה של מדינה. תמיר פרדו, ראש המוסד לשעבר, סבור כי "הסייבר הפך למקבילה השקטה של נשק גרעיני ולנשק האולטימטיבי שיכול פשוט לפרק מדינות. צבאות נועדו להגן על גבולות לאומיים, אבל הגבולות הפכו חסרי משמעות, ושדה הקרב עבר במידה רבה מהזירה הצבאית לאזרחית".[4] ואומנם תקיפות סייבר על תשתיות אזרחיות ועל יכולות חיוניות אחרות עלולות להסב נזק הרסני יותר ממתקפה גרעינית. פצצות גרעיניות הן הרסניות, אבל ההשפעות שלהן הן מקומיות, או אזוריות אם שולבו עם אמצעים צבאיים. ההשפעות הקטלניות של נשקי סייבר יהיו איטיות יותר, אבל עלולות להיות מערכתיות.[5] תקיפות סייבר הן למעשה מלחמה באמצעים אחרים.

לדוגמה, אם מתקפת סייבר תצליח להשבית את רשת החשמל של מדינה או אפילו רק חלקים מרכזיים שלה, היא תוכל לשתק את הכלכלה ואת הצבא של המדינה ולעצב את תוצאת העימות. תקיפות נגד מערכות מים, תקשורת או תחבורה עלולות לגרום לקטל המוני מקור, מהתייבשות, מתאונות דרכים ומתקלות חמורות בתחבורה. הן יכולות להוריד רכבות מן הפסים, להשבית רמזורים או להשתלט על מטוסי נוסעים מסחריים בעת הטיסה. תקיפות סייבר יכולות להשתלט על מערכות הניטור של כורים גרעיניים, בתי זיקוק או מפעלים כימיים, ולגרום להשבתתם או לגרוע מכך. תקיפות על מוסדות פיננסיים יכולות להעביר כספים בין חשבונות או למנוע גישה לחסכונות ולהשקעות, מה שיוביל לכאוס כלכלי. רישום אוכלוסין ומקרקעין, מאגרי מידע אוניברסיטאיים, שרשראות הפצה של מוצרים חקלאיים ושל מזון, מערכות לייצור רכב, אלקטרוניקה ותרופות ומערכות למענה בחירום – כולם יהיו בסכנת שיבוש או השבתה.

4 תמיר פרדו, ריאיון עם המחבר.

5 Joseph S. Nye, *The Future of Power: Its Changing Nature and Use in the Twenty-first Century* (New York: Hachette Book Group, 2011), 212; Jeremy Straub, "Hackers Could Kill More People than a Nuclear Weapon," *LiveScience.com*, August 27, 2019; United States Subcommittee on Emergency Preparedness, Response and Communications and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies (2014); Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (HarperCollins, 2010).

אחת ההשפעות המובהקות של הסייבר היא על איסוף מודיעין ועל מבצעי מודיעין. בעבר נאלצו סוכנויות ביון להקדיש משאבים רבים לפיתוח של נכס בודד. בשנת 2020 פגעה רוגלה רוסית בעשרות מטרות רגישות, חלקן ביטחוניות, בארצות הברית, בקנדה, במקסיקו, בבריטניה, בבלגיה, בספרד, באיחוד האמירויות ובישראל.[6] פצחנים המזוהים עם סין ביצעו תקיפות סייבר מסיביות נגד חברות טכנולוגיה ומוסדות פיננסיים בארצות הברית, ביפן ובאירופה, ונזקן הוערך בטריליוני דולרים.[7]

תחום הסייבר הפך לאמצעי חשוב לשמירה על הסדר בתוך מדינה. "חומת האש הגדולה של סין" משמשת לשליטה בגישה של משתמשים מקומיים לאינטרנט ולמעקב אחריה. סין משתמשת גם בבינה מלאכותית, בתוכנות לזיהוי פנים ובטלפונים סלולריים כדי לנהל מעקב גלובלי אחר יריביה הפוליטיים. ברוסיה ניהול תעבורת האינטרנט המקומית הוא ריכוזי, וברשת המקומית יש "נקודות חנק" (chokepoints) שנועדו לחסום גישה לרשת העולמית. איראן משתמשת בקמפיינים של מעקב סייבר כדי לרגל אחר מתנגדי משטר בחו"ל וכדי לדכא את האופוזיציה המקומית.[8] רבים מן המתכנתים ומן היצרנים של התוכנות ושל החומרות המשמשות כמעט את כל המכשירים האלקטרוניים (מחשבים, טלפונים חכמים, מכשירים רפואיים, מכוניות, טילים, מטוסים וכו') חיים במדינות שמשטרן סמכותני. המצב הזה מגדיל את הסיכוי שגורמים אלה יתקינו קוד נסתר במוצרים שלהם למטרות ריגול או הרס.

מבצעי תודעה בסייבר, בעיקר נגד מערכות בחירות במערב, הם אפקטיביים במיוחד. מבצעי סייבר סיניים כוונו נגד הקמפיינים לנשיאות של ברק אובמה ושל ג'ון מקיין כבר ב־2008, ושל ג'ו ביידן ב־2020.[9] התקיפה הרוסית על הבחירות לנשיאות ארצות הברית ב־2016 הייתה כנראה מבצע הסייבר הידוע ביותר שנערך אי פעם. ייתכן שהוא היה חלק

6 David E. Sanger, Nicole Perlroth, and Julian E. Barnes, "As Understanding of Russian Hacking Grows, So Does Alarm," *New York Times*, January 2, 2021.

7 Zolan Kanno-Youngs and David Sanger, "U.S. Accuses China of Hacking Microsoft," *New York Times*, July 19, 2021; Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Age* (New York: Public Affairs, 2017), 8.

8 Segal, *Hacked World Order*, 7–9; U.S. Cyberspace Solarium Commission, Report (March 2020), 9-10, 17; Laura Rosenberger, "Making Cyberspace Safe for Democracy." *Foreign Affairs* (May/June 2020); Ronen Bergman and Farnaz Fassihi, "Iranian Hackers Found Way Into Encrypted Apps, Researchers Say," *New York Times*, September 18, 2020.

9 David E. Sanger, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age* (New York: Crown, 2018), 18; Tim Starks, "Russia, China and Iran Trying to Hack Presidential Race, Microsoft Says," *Politico*, September 10, 2020.

ממאמץ אסטרטגי רחב שנערך ב־19 מדינות ונועד לפצל את המחנה המערבי, להחליש את נאט"ו ולערער את האמון בתהליכים ובמוסדות דמוקרטיים.[10]

ידוע רק על מקרה אחד שבו לתקיפת סייבר הייתה השפעה קטלנית ישירה, אך תקיפות סייבר גרמו שוב ושוב לנזק פיזי, והיכולת שלהן רק הולכת וגדלה. גם אם רוב תקיפות הסייבר נכשלות, מספרן עצום ולכן גם ההצלחות הבודדות הצפויות להן עשויות להספיק כדי לערער את אמון הציבור במערכת לאומית או בינלאומית מסוימת. טכנולוגיית סייבר, מומחיות בסייבר ונשק סייבר זמינים לרכישה בשוק שחור מקוון ופורח. במחיר לא גבוה אפשר לרכוש יכולת בסיסית, וכמה מן היכולות המתוחכמות מסוגלות לחדור אפילו למערכות ממשלתיות ומסחריות מוגנות היטב. מידע שנגנב מממשלות ומגופים פרטיים זמין גם הוא לרכישה. חברה אחת אפילו מספקת מסד נתונים ובו המיקום וכתובות האינטרנט של מאות מיליוני מחשבים פגיעים ברחבי העולם ומציעה חבילות יעדים לתקיפה.[11]

התלות העמוקה בסייבר של שחקניות מדינתיות המתאפיינות בקדמה טכנולוגית היא בכל תחומי החיים המודרניים, והיא מספקת ליריבים מדינתיים ולא מדינתיים חלשים מגוון הזדמנויות לחולל נזק. תקיפות סייבר הן אטרקטיביות במיוחד מכיוון שהן בדרך כלל זולות יותר מן הקינטיות, מספקות אנונימיות ויכולת הכחשה שבתקיפה מסוג אחר קשה להשיג, והן אינן זקוקות לטריטוריה או לתשתית לאומית. תקיפה מתמשכת על רשתות אינטרנט מסחריות או ממשלתיות שאינן מוגנות דיין עלולה לכרסם אט־אט בכלכלה הלאומית ובמורל הציבורי ולכפות על היריב ויתורים שאינם רצויים לו. עם זאת, לרוב השחקנים האלה אין את

10 Daisuke Wakabayashi and Scott Shane, "Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election," *New York Times*, September 27, 2017; Craig Timberg and Tony Romm, "New Report on Russian Disinformation, Prepared for the Senate, Shows Operation's Scale and Sweep," *Washington Post*, December 17, 2018; Julian Barnes, "Russians Tried, but Were Unable to Compromise Midterm Elections, U.S. Says," *New York Times*, December 21, 2018.

11 Shane Harris, *@War: The Rise of the Military-Internet Complex* (Eamon Dolan/Mariner, 2014), 103–105; Chris Bing, "Chinese-authored Spyware Found on More than 700 Million Android Phones," *Cyber Scoop*, November 15, 2016; Jeremy Hsu, "U.S. Suspicions of China's Huawei Based Partly on NSA's Own Spy Tricks," *IEEE Spectrum*, March 26, 2014; Stan Schroeder, "CIA, FBI, NSA: We Don't Recommend Huawei or ZTE Phones," *Mashable*, February 14, 2018; The Economist, "The WannaCry Attack Reveals the Risks of a Computerised World," May 20, 2017; Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data* (Santa Monica: Rand Corporation, 2014), ix, 370.

היכולת הנדרשת כדי לחדור ליעדים מוגנים היטב. לשם כך נדרשת יכולת להקים צוותים מקצועיים רבים בעלי מגוון מיומנויות המסוגלים לפתח תקיפות על מערכות יעד ספציפיות. זהו תהליך עתיר משאבים וזמן.[12]

ארגוני טרור משתמשים בסייבר לתכנון מבצעי, לגיוס אנשים, להדרכה, לגיוס כספים, לתקשורת, לריגול, לתעמולה ולמבצעי תודעה. אל־קאעדה, דאעש וארגוני טרור אחרים הצהירו מפורשות על רצונם להשתמש בתקיפות סייבר כדי לגרום לנזק פיזי ישיר.[13]

מה מייחד את הסייבר?

תחילה כמה הגדרות קצרות.

תקיפות על רשתות מחשבים (Computer Network Attacks, CNA) משבשות מערכות ורשתות מחשב, פוגעות בהן, מונעות גישה אליהן, משחיתות ואפילו משמידות אותן (כלומר חבלת סייבר), ועשויות לשמש למטרות הרתעה.

תקיפות לניצול רשתות מחשבים (Computer Network Exploitation, CNE) חודרות בחשאי למערכות מחשב ותקשורת כדי לאסוף מידע, לשנות או למחוק אותו (כלומר ריגול סייבר), ומשמשות למבצעי מודיעין ולדיכוי התנגדות פנימית.

תקיפות השפעה על רשתות מחשבים (Computer Network Influence, CNI), נקראות גם "מבצעי תודעה בסייבר", פועלות על מידע ועל אמצעי תקשורת כדי להשפיע על תפיסותיהם של יחידים, של קבוצות או של הציבור הרחב, בתוך המדינה או מחוצה לה. הן יכולות לשמש לקידום מטרות פוליטיות, לשיבוש מערכות בחירות ואף לערעור הלגיטימיות והיעילות של ממשלה.

12 Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law and Policy* 4, no. 63 (2010): 66; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 378–379, 396–397; Ivanka Barzashka, "Are Cyber-Weapons Effective?" *The RUSI Journal* 158, no. 2 (2013): 51; Trey Herr, "PrEP: A Framework for Malware & Cyber Weapons," *Cyber Security Policy and Research Institute*, George Washington University (March 12, 2014): 8.

13 Lin, "Offensive Cyber Operations," 66; Lindsay, "Stuxnet and the Limits of Cyber Warfare," 378–379, 396–397; Barzashka, "Are Cyber-Weapons Effective?" 51; Herr, "PrEP," 8; Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World," *Orbis* 59, no. 1 (2015): 123; Yoram Schweitzer, Gabi Siboni, and Einav Yogev, "Cyberspace and Terrorist Organizations," *Military and Strategic Affairs* 5, no. 3 (2013): 21.

מבחינות רבות תקיפות סייבר דומות לתקיפות קינטיות בעולם הפיזי, ואפשר להתמודד איתן באמצעות יישום גישות ואסטרטגיות דומות. עם זאת, לתקיפות סייבר יש כמה מאפיינים שבגינם ראוי לראות בהן תחום נפרד של עימות המחייב טיפול שונה.

הבדל חשוב ראשון בין תקיפות קינטיות לתקיפות סייבר הוא המהירות שבה הן מתרחשות. תקיפות סייבר מתרחשות כהרף עין, דבר שמקשה על הכנת הגנות מפניהן, מלבד הגנות אוטומטיות, ומונע ממקבלי ההחלטות את הזמן הדרוש לגיבוש תגובה שקולה. מנגד, כמה מן השלבים של תקיפות סייבר מתוחכמות מתחוללים במהירות של בני אנוש, לאורך חודשים ואף שנים, ובכלל זה תכנון התקיפות, איסוף מודיעין, פיתוח קוד מותאם למערכות יעד ספציפיות והיערכות מבצעית.[14]

גם למדינות חזקות ומתקדמות טכנולוגית אין מונופול על השימוש בכוח בסייבר. תקיפות קינטיות יכולים לבצע שחקנים מדינתיים או ארגוני טרור; כל מי שמצויד במחשב יכול לבצע תקיפת סייבר ולגרום ולו למידה מסוימת של נזק. חלק מיכולות המחשוב המתקדמות ביותר, שבעבר היו שייכות אך ורק לשחקנים מדינתיים ולתאגידים גדולים, נגישות כעת לכול. מדינות חלשות או שחקנים לא מדינתיים בעלי ממון יכולים לפתח יכולות סייבר צבאיות עוצמתיות ולהשיג תוצאות חסרות תקדים.[15]

בניגוד לכל כלי הנשק האחרים, קונוונציונליים או לא קונוונציונליים, לאמצעי הלחימה בסייבר אין מגבלות גיאוגרפיות ואין אילוצי זמן ומרחב. אפשר לשגר אותם בו־זמנית ברחבי העולם נגד מספר בלתי מוגבל של מטרות ולחצות באמצעותם גבולות בלי שמדינות ידעו אפילו שהרשתות שלהן נפרצו ושריבונותן הופרה.[16]

14 Clarke and Knake, *Cyber War*, 31; Ben Buchanan *The Cyber Security Dilemma: Hacking, Trust, and Fear between Nations* (New York: Oxford, 2017), 42.

15 Lucas Kello, "The Meaning of the Cyber Revolution," *International Security* 38, no. 2 (2013): 36; Jonathan Silber, "Cyber Vandalism – Not Warfare," *Ynet*, January 26, 2012; R. Bebber, "Information War and Rethinking Phase 0." *Journal of Information Warfare* 15 no. 2 (2016): 39–52; F. J. Cilluffo and J. R. Clark, "Building a Conceptual Framework for Cyber's Effect on National Security," *Journal of Information Warfare* 15, no. 2 (2016): 7; Segal, *Hacked World Order,* 12.

16 Eviatar Matania, Lior Yoffe, and Michael Mashkautsan, "A Three Layer Framework for a Comprehensive National Cyber-Security Strategy," *Georgetown Journal of International Affairs* 27, no. 3 (2016): 77–84; Clarke and Knake, *Cyber War*, 31; Kello, "The Meaning of the Cyber Revolution," 22.

לכל מערכות הנשק, אפילו הגרעיניות, יש השפעה מקומית בלבד; אולם לתקיפות סייבר עשויה להיות השפעה מערכתית או כלל־ארצית. תקיפה קינטית מצד שחקן מדינתי או לא מדינתי עלולה להשמיד בנק, בית חולים, מכ"ם או מתקן תקשורת צבאי. תקיפת סייבר, לעומת זאת, עלולה להפיל מערכת פיננסית או מערכת בריאות שלמה, לקלקל ולשבש את מערכות ההתרעה המוקדמת ואת מערכות הפיקוד והשליטה של האויב ולפגוע ביכולתו להגיב. שיבוש כלל־ארצי או אפילו אזורי בלבד של רשת החשמל של היריב עלול לגרום לכאוס חברתי, כלכלי וצבאי.[17]

בניגוד לתקיפות קינטיות, נדיר שתקיפות סייבר יגרמו לנזק פיזי ישיר או לאובדן חיים, וריגול סייבר יכול להתבצע מרחוק בלי לסכן את חיי המרגלים. את רמת הדיוק של נשק הסייבר קשה להשיג בתקיפות קינטיות, ולכן אפשר למזער את הנזק היקפי שלו גם כאשר המטרות נמצאות בלב אוכלוסייה אזרחית. אפשר לתכנן מראש שההשפעות של נשק הסייבר יהיו זמניות או הפיכות. עם זאת, ההשפעות העקיפות של נשק הסייבר עלולות לגרום לנזק פיזי וקטלני נרחב.[18]

ייחוס תקיפה קינטית לשחקן מדינתי או לא מדינתי הוא בדרך כלל פשוט וברור. תקיפות סייבר אפשר להסוות ביתר קלות, ואפשר להסב באמצעותן נזק בלי להשאיר עקבות. אפשר שהיעד לתקיפה אפילו לא ידע שהותקף. עם זאת, מדינות ואפילו חברות פרטיות שיפרו מאוד בשנים האחרונות את יכולות המודיעין הטכנולוגיות והפורנזיות שלהן, ובעקבות זאת את היכולת שלהן לזהות מי עומד מאחורי מתקפה.[19]

17 Constance Douris, "Cyber Assault on Electric Grid Could Make U.S. Feel Like Post-Hurricane Puerto Rico," *Forbes*, February 6, 2018.

18 Thomas Rid, *Cyber War Will Not Take Place (*London: C. Hurst and Co, 2013), viii; Jan Trobisch, *Challenges in the Protection of US Critical Infrastructure in the Cyber Realm* (School of Advanced Military Studies, US Army Command and General Staff College, Fort Leavenworth, KS, 2014), 4; David E. Sanger, "Why Hackers Aren't Afraid of Us," *New York Times*, June 16, 2018; George Perkovich and Ariel (Eli) Levite, eds. *Understanding Cyber Conflict: 14 Analogies* (George University Press, 2017), 45, 116; Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2018): 382.

19 Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 (Tel Aviv: INSS, 2012), 32–33; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Rand Corporation, 2009), xiv-xv; Clarke and Knake, *Cyber War,* 45, 51; Silber, "Cyber Vandalism – Not Warfare"; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks." *The Journal of Strategic Studies* 38, no. 1–2 (2015): 7.

כלי הנשק הקונוונציונליים והבלתי קונוונציונליים יכולים לשמש נגד מגוון רחב של מטרות, אולם נשק סייבר מתוחכם (שאינו אלא קוד מחשב) מיועד לתקוף מטרה מסוימת, ודי בשינויים קלים במטרה כדי שיהפוך לחסר תועלת. לדוגמה, קוד שפותח כדי לתקוף מערכת טילי קרקע־אוויר מסוימת לא יועיל נגד מערכת אחרת מאותו סוג או נגד מערכת טילי אוויר־אוויר.[20]

בעבר נאלצו סוכנויות ביון להתאמץ ולהסתכן כדי לאסוף מידע מסווג ואפילו לא מסווג. כיום, בעזרת מערכות נתוני עתק (ביג דאטה), הן מסוגלות לעבד כמויות אדירות של מידע לא מסווג; כל פרט מפרטיו אולי שולי, אך מכולם יחד אפשר להפיק מידע חיוני. מדינות רבות מנהלות זה מכבר מבצעי תודעה; הסייבר מציע מגוון פלטפורמות שאפשר להגיע דרכן ישירות, מיידית ובזול למספר עצום של אנשים ברחבי העולם או לקהלים ממוקדים במיוחד.

20 Martin C. Libicki, "Second Acts in Cyberspace," in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Brookings, 2019), 137; Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Brookings, 2019), 121.