טכנולוגיית הרשתות הסלולריות מהדור החמישי (5G) ופריסתן בישראל: יתרונות, איומים וצעדים להמשך

עמרי וקסלר ודורון פלדמן

נובמבר 2020

ICRC
Blavatnik Interdisciplinary Cyber Research Center

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

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

הקדמה

בסוף חודש ספטמבר 2020 העניק משרד התקשורת לחברות התקשורת רישיונות לשימוש בתדרים עבור רשתות תקשורת סלולרית מהדור החמישי (5G), שפריסתן המלאה בארץ תושלם ככל הנראה עד 2024. לטכנולוגיית ה-5G צפויות השלכות רבות, לא רק בתחום התקשורת אלא גם בתחומי הרפואה, החינוך והביטחון והיא צפויה להוות בסיס להתפתחות ענפים טכנולוגיים מתקדמים כגון ערים חכמות ותחבורה אוטונומית.

מסיבה כזו או אחרת הקדימו החברות הסיניות את החברות המערביות בפיתוח תשתיות תקשורת 5G. על רקע התחרות הכלכלית והטכנולוגית בין ארה"ב וסין, הפכה לכן רכישתן ופריסתן של תשתיות תקשורת מתקדמות אלו, לנושא המעורר עניין רב בתקשורת. עניין זה התעצם עם דרישתה של ארה"ב מבעלות בריתה, וביניהן ישראל, שלא לרכוש טכנולוגיות תקשורת מתוצרת סין. ההתמקדות בנושא רשתות ה-5G על רקע המאבק המעצמתי הובילה למתן תשומת לב מועטה בלבד לסוגיות חשובות אחרות הנוגעות לטכנולוגיה המתקדמת.

המאמר שלהלן סוקר את חשיבות טכנולוגיית רשתות ה-5G, יתרונותיה וההזדמנויות שהיא מביאה עמה לעומת איומי הסייבר והאיומים על הפרטיות הנלווים לשימוש בה. לבסוף, מציע המאמר דרכי פעולה אפשריות למקבלי ההחלטות בישראל להטמעת הטכנולוגיה תוך התמודדות עם חולשותיה הפוטנציאליות.

פרופסור יצחק בן ישראל

ראש סדנת יובל נאמן למדע, טכנולוגיה וביטחון

ראש המרכז הרב-תחומי לחקר הסייבר ע"ש בלווטניק

* המחברים מבקשים להודות לחוקרי הסדנה הבכירים, פרופ' יצחק בן-ישראל ופרופ' עוזי ארד, על ההשראה, ועל הנכונות לשתף בידע, ללמד ולייעץ – כל אלה תרמו מאוד לתהליך כתיבת המאמר.

מבוא

בשנים האחרונות טכנולוגיית הדור החמישי של רשתות התקשורת הסלולרית (5G) עלתה לכותרות והכתה גלים בעולם ובישראל. על פי ההערכות צפויה טכנולוגיה פורצת דרך זו להוביל למהפכה ולשנות מהיסוד את כל אורחות חיינו. הטכנולוגיה תסייע לקדם את פיתוחם של רכבים אוטונומיים וערים חכמות ותתמוך בפתרונות טכנולוגיים בתחומי התקשורת, הרפואה והחינוך. נוסף על כך היא עשויה להשפיע על תהליכי קבלת החלטות ברמות המדיניות והאסטרטגיות הגבוהות ביותר, לתרום לצמיחה ולרווחה הכלכלית של מדינות ולהוביל לשינוי פני המערכות הצבאיות ושדה הקרב. לפי תחזיות שונות, מדינות אשר יקדמו בברכה את תשתיות התקשורת המתקדמות, ובהן רשתות 5G, יוכלו להתכונן בצורה טובה יותר לאתגרי העשור הקרוב.

רכישתן של תשתיות התקשורת המתקדמות נמצאת במרכז מאבק המעצמות ארצות הברית וסין; מאבק זה מתבטא, בין השאר, בדרישתה של ארצות הברית מבעלות בריתה – ובהן ישראל – להימנע מלהתקין טכנולוגיות תקשורת מתוצרת סין או להשתמש בהן. הדיון בדרישה זו עמד במרכז סדר היום בישראל ובעולם, ובשל כך זכו סוגיות חשובות אחרות הנוגעות לטכנולוגיה המתקדמת לתשומת לב מוגבלת למדיי. במאמר זה נבקש לגשר על הפער הקיים ולבחון מתוך נקודת מבט רחבה את ההשלכות האסטרטגיות של פריסה והטמעה של טכנולוגיית 5G בישראל. ננסה להשיב לשלוש שאלות: מהן רשתות 5G ומהם שימושיהן העיקריים? מדוע הן חשובות ונחוצות לביטחונה הלאומי של ישראל? מהם האיומים האפשריים הנלווים לשימוש ברשתות וכיצד אפשר להתמודד איתם?

תחילה נסקור את חשיבות הטכנולוגיה ויתרונותיה, את ההזדמנויות שהיא מביאה עימה, את השימושים שהיא עתידה לאפשר ואת השפעתה הצפויה על ביטחונה הלאומי של ישראל במובן הרחב. בהמשך נדון באיומי הסייבר ובאיומים על הפרטיות הנלווים לשימוש בטכנולוגיית 5G. לבסוף נציע דרכי פעולה אפשריות למקבלי ההחלטות בישראל להטמעת הטכנולוגיה ולהתמודדות עם חולשותיה הפוטנציאליות.

טכנולוגיית 5G ותרומתה לחדשנות ולביטחון הלאומי של ישראל

רקע – תפיסת הביטחון הלאומי של ישראל

דוד בן-גוריון סבר כי כדי לצמצם את הפער המובנה בין ישראל לבין העולם הערבי, על כוחות הצבא של ישראל לעלות על אלה של אויביה בכושר המחשבה, בכושר הלחימה ובכוח הסבל. בעת שגיבש בן-גוריון את תפיסת הביטחון של ישראל בסיומה של מלחמת העולם השנייה, הוא סבר כי יש לטפח את עקרון האיכות, שממנו נגזר הצורך לשמר ולהעצים את היתרון הטכנולוגי היחסי של ישראל לעומת צבאות ערב: פיתוח אמצעי לחימה מתקדמים והתמקדות בחיל האוויר, כוח המחץ של צה"ל (בן-ישראל, 2013).

עקרון המפתח של השקעה באיכות מצוי במרכז תפיסת הביטחון שגיבש בן-גוריון ומתמקד בצורך להשקיע בגורם האנושי, כלומר לטפח את המצוינות, החינוך, ההשכלה הגבוהה, המדע והטכנולוגיה ('הגניוס היהודי') כדי ליצור חברה פתוחה המבוססת על ידע. להשקעה בעקרון האיכות היו שתי תכליות עיקריות: לשמש אמצעי לפיתוח הארץ וכלכלתה ולפיתוח עוצמתה הביטחונית של ישראל (בן-ישראל, 2013).

תפיסתו של בן גוריון עדיין נוכחת ומלווה את ההוויה והעשייה הביטחונית, האזרחית והכלכלית של ישראל. אולם במרוצת המאה העשרים הלכה והתרחבה משמעות המושג ביטחון לאומי אל מעבר להיבט הצבאי-ביטחוני הצר. במובנו הרחב מתייחס המושג ליכולתה של מדינה לרתום את כלל משאביה ואמצעיה הלאומיים בזירות שונות – צבא, כלכלה, חברה, מדע, טכנולוגיה וחינוך – כדי לגייסם להגשמת היעדים הלאומיים המרכזיים וארוכי הטווח של האומה והעם.[1] למרות זאת, מלאכת מחשבת חשובה ודומה לזו שעשה בן-גוריון ברגעיה המכוננים של מדינת ישראל הצעירה לא נעשתה עד כה, ולפיכך ישראל נעדרת תפיסת ביטחון עדכנית המותאמת לאתגרים הביטחוניים-מדיניים, הכלכליים והחברתיים העומדים לפתחה במאה העשרים ואחת.

חשיבותה של טכנולוגיית הדור החמישי

בשנים האחרונות אנו עדים להתפתחותה של טכנולוגיית הדור החמישי (5G) של רשתות התקשורת הסלולרית ולהתגברות סיקורה בתקשורת. על פי ההערכות, פריסתה והטמעתה של הטכנולוגיה עתידות לגרום לשינוי מהפכני. בהשוואה לדורות התקשורת הקודמים, 3G ו-4G, רשתות 5G ייחודיות בכך שהן צפויות לאפשר שימוש במגוון טכנולוגיות (כגון הגדלת טווח התדרים, ריבוי אלומות ו-MIMO)[2] וכלים עתידניים, להגביר במידה ניכרת את המהירות וההיקף של העברת הנתונים, לקצר את זמן ההמתנה (latency) להעברתם, לאפשר חיבור מכשירים רבים יותר לרשת ועוד. כל אלה צפויים לאפשר את פיתוחן של טכנולוגיות חדשות (כגון ערים חכמות ותחבורה אוטונומית) ושל מודלים עסקיים ותחומי תעשייה חדשים. למעשה, רשתות 5G עשויות לשנות את כל אורחות חיינו – לא רק בתחום התקשורת אלא בתחומים נוספים כמו רפואה וחינוך, להשפיע על תהליכי קבלת החלטות ולהוביל לשינוי בדפוסי הפעלת הכוח

1 עלייתו של המושג 'אסטרטגיית-על' (Grand-Strategy), המתאר את הרמות הגבוהות ביותר של אסטרטגיה ומדינאות, החלה במלחמת העולם הראשונה ומזוהה עם כתביהם של Fuller, Liddell Hart, Earle, Brands, Kennedy ואחרים (מוסד שמואל נאמן, 2017, עמ' 28–29).

2 MIMO (Multiple Input – Multiple Output) היא טכניקה להגברת אותות הרדיו באמצעות שימוש במספר רב של אנטנות שידור וקליטה.

של מדינות בעת עימותים. אם כן, מדינות אשר ישכילו לאמץ בהקדם את תשתיות התקשורת המתקדמות ביותר יוכלו להתאים את עצמן ולהתכונן בצורה טובה יותר לעשור הקרוב ולאתגרים שיביא עימו (Burnham, 2019; Eurasia Group, 2018; Jones, 2019; Oxford Economics, 2019).

מדינות רבות החלו לפרוס רשתות 5G באופן ראשוני בשנים 2018–2019, ומהלך זה צפוי להגיע לשיאו משנת 2025 ואילך (Eurasia Group, 2018, p. 9). לעומת זאת, בישראל נמצא תהליך פריסת רשתות 5G והטמעתן רק בראשיתו. ככלל, ישראל מפגרת בעניין זה אחר שאר מדינות העולם; כך, למשל, פריסת רשתות הדור הרביעי (4G) – החלה רק בשלהי שנת 2015 (פרץ, 2020), אף שטכנולוגיה זו הייתה קיימת עשור אחד קודם לכן (Duffy, n.d., p. 7).

כדי שישראל תוכל לשמר את עוצמותיה לאורך זמן, להעצים את יתרונותיה היחסיים ולממש בכך את יעדיה הלאומיים, יהיה עליה להאיץ את פריסתה והטמעתה של טכנולוגיית 5G – מתוך ראייה ארוכת טווח ובזהירות הנדרשת. ככל שישראל תצעד בכיוון זה כך תגבר יכולתה לשמור על מעמדה כאומת סטארט-אפ (ינובסקי, 2020) ועל יכולותיה בתחומי הטכנולוגיה והחדשנות (כהן, 2018, עמ' 2), תחומים שבהם יש לה יתרון יחסי מובנה[3] – לעומת מדדי עוצמה לאומית אחרים שבהם היא משתרכת מאחור.[4]

הצטיינותה של ישראל בתחומים אלה אינה מובנת מאליה, ויש לראותה כ"תהליך בלתי נגמר, משתפר ומשתנה" (לוי, 2016). הרצון לשמר את יתרונה של ישראל, במיוחד בעידן המתאפיין בתחרות גלובלית ובמרוץ עולמי לשליטה בתחומי הידע הטכנולוגיים, בבלוקצ'יין (Blockchain), במחשוב הקוונטי, בבינה המלאכותית ובמערכות אוטונומיות אחרות (לוצאטו, 2019) – הופך את פריסתה הנרחבת של טכנולוגיית 5G ואת הטמעתה לחיוניות.

יתרה מזו, פריסה והטמעה של טכנולוגיה מתקדמת הכרחית עבור מדינה קטנה כישראל, המתבססת במידה מועטה יחסית על תעשיות מסורתיות[5] (החדשנות הטכנולוגית כמנוע צמיחה מרכזי של ישראל, ל.ת.), נתונה לאיום תמידי ומתמודדת מדי יום עם אתגרים המחייבים אותה להקדים את אויביה בכמה צעדים. על כן, ברמה הצבאית-ביטחונית, המעבר לטכנולוגיית 5G והסתמכות על יכולותיה להעביר ולעבד כמויות גדולות של נתונים יאפשרו לשפר במידה ניכרת את פיתוח אמצעי הגנת הסייבר, את הפעלתם של אמצעי לחימה אוטונומיים ואת התקשורת

3 הצטיינותה של ישראל בתחום זה בולטת בקרב גופי המחקר המובילים המדרגים מדי שנה את מדינות העולם לפי מידת החדשנות שלהן. ראו למשל את דוח הכלכלות התחרותיות הגלובלי (Global Competitiveness Report) של הפורום הכלכלי העולמי (World Economic Forum) לשנת 2019, שבו דורגה כלכלת ישראל במקום העשרים מתוך 141 מדינות: בתת-מרכיב "דינמיות עסקית" דורגה ישראל במקום החמישה-עשר ובתת-מרכיב "יכולת חדשנות" – במקום הרביעי (Schwab, 2019). עוד ראו את מדד החדשנות הגלובלי (Global Innovation Index) שמפרסמים במשותף אוניברסיטת קורנל, בית הספר למנהל עסקים INSEAD והארגון העולמי לקניין רוחני באו"ם (WIPO), שבו דורגה ישראל ב-2019 בתחום החדשנות במקום העשירי מ-129 מדינות. במדד צוינה לחיוב הצטיינותה של ישראל בכמה תת-מרכיבים, בהם למשל פיתוח אפליקציות (מקום ראשון), פיתוח פטנטים (מקום שני), תעסוקת נשים בעלות תארים מתקדמים (מקום שלישי) ושיתופי פעולה בתחום המחקר בין התעשייה לאקדמיה (מקום שני) (Dutta, Lanvin, & Wunsch-Vincent, 2019).

4 ראו למשל, את שיעורי העוני ואי השוויון הגבוהים בישראל באופן יחסי למערב (וייס, 2020); את דירוגה הנמוך של ישראל במדד פיז"ה של ה-OECD לשנת 2018 (מכ-80 מדינות דורגה ישראל בשנת 2018 במתמטיקה – במקום 42, במדעים – במקום 43 ובקריאה – במקום 38) (OECD, 2019); ואת מדד השחיתות שמפרסם ארגון Transparency International, שבו דורגה ישראל בשנת 2019 במקום ה-35 מ-180 מדינות (Transparency International, 2020, p. 2).

5 על-פי הגדרות הלמ"ס, תעשייה מסורתית ומסורתית-מעורבת כוללת ייצור מזון ומשקאות, טקסטיל והלבשה, מתכת ומוצריה, חומרי בניין ועוד (התעשייה המסורתית מתחברת לחדשנות, ל.ת.).

בשטח (בן פורת, 2020), את יכולת הפיקוד והשליטה, את היכולות בתחומי המודיעין, המעקב ואיסוף המל"ם,[6] את התחזוקה והלוגיסטיקה, את הגנת הגבולות ועוד (Hoehn & Sayler, 2020). נוסף על תרומתה לתחום הביטחון צפויה טכנולוגיית 5G להשפיע גם על החברה בתחומים כגון עוצמה כלכלית-חברתית, ענף הרפואה, החינוך ומעמדה האזורי והבין-לאומי של ישראל – ועל כך להלן.

עוצמה כלכלית-חברתית

פריסה והטמעה של טכנולוגיית 5G עשויות לתמוך בתהליכי דיגיטציה חברתיים-כלכליים בתחומים בעלי חשיבות אסטרטגית-לאומית: ניידות ותחבורה חכמה, חקלאות חכמה, ניהול משק אנרגיה חכם, צמיחה כלכלית וצמצום פערים חברתיים.

ניידות ותחבורה חכמה

טכנולוגיית 5G אמורה לסלול את הדרך לשימוש גובר יותר בכלי רכב אוטונומיים או כאלה הנשלטים מרחוק באמצעות רשת תקשורת, משום שהיא תאפשר להם לאסוף בזמן אמת נתונים מהסביבה החיצונית – מרמזורים, מרכבים אחרים, מחיישנים שיוטמעו לאורכן של דרכים, מהולכי רגל וממשתמשים בתחבורה הציבורית. נתונים אלה יאפשרו לייעל את התעבורה ולחסוך משאבים וזמן באמצעות זיהוי מפגעי דרך ומזג אוויר, הפחתת גודשי תנועה וויסות מקומות חניה, וכך יובילו לצמצום טעויות אנוש וייתכן שאף לצמצום תאונות הדרכים. איסוף כזה של נתונים וניתוחם בזמן אמת יאפשרו לתכנן דרכים ומסלולי תחבורה ציבורית חדשים, לנהל את הביקוש לתחבורה הציבורית ולשפר את זמינותה, לקצר את זמני הנסיעה בכלי רכב וכפועל יוצא לצמצם את פליטתם של גזי חממה. הם יאפשרו לנהל ציים לוגיסטיים חכמים שיהפכו את התעבורה בדרכים לנוחה יותר גם במצבי חירום. שימוש ברכבים אוטונומיים עשוי לשפר את ניודם של מבוגרים ושל בעלי מוגבלויות שאינם נוהגים בכוחות עצמם, וכך להקל עליהם להשתלב בשוק העבודה (Aria et al., 2020, p. 16; Duffy, n.d., pp. 9–10; Federal Ministry of Transport and Digital Infrastructure, 2017, p. 10; GSMA, 2018, p. 47). לבסוף, 5G וטכנולוגיות מחשוב מתקדמות דוגמתה יכולות לסייע להתמודד עם הביקוש ההולך וגובר מצד עסקים ואזרחים לאספקת מוצרי מזון ומוצרי צריכה ללא מגע אדם, צורך שהודגם בצורה בולטת בעת משבר הקורונה (KPMG, 2020, p. 9).

חקלאות חכמה

טכנולוגיית 5G תתמוך בשיפור ובייעול של ענף החקלאות. כך, למשל, יכולותיה של הטכנולוגיה לאפשר העברת כמויות גדולות של נתונים במהירות, ולחבר מכשירי IoT (האינטרנט של הדברים) רבים, תאפשר זרימת מידע מחיישנים שיותקנו באדמה ויסייעו למדוד טמפרטורה ואחוזי לחות ולזהות מחלות ומזיקים שיש להם פוטנציאל לפגוע ביבול החקלאי. היא תאפשר לנטר את היבול בזמן אמת כדי לזהות מגמות בתהליך הגידול. פריסתה תאפשר לבצע ניטור

6 ISR – Intelligence, Surveillance and Reconnaissance.

ומעקב תמידי אחר משק החי, בין השאר באמצעות שימוש ברחפנים שישדרו לחדר בקרה מרכזי אחד. באותו אופן יתאפשר לשלוט מרחוק במיכון חקלאי אוטומטי ולוודא כי הוא פועל היטב, וכך להגביר את היעילות ולחסוך בכוח אדם. טכנולוגיית 5G תוכל לתרום גם לצמצום עלויות התפעול באמצעות מעבר למערכת השקיה חכמה, שבעזרת בקרים תימנע בזמן אמת שימוש בזבזני במים (Little, 2017, p. 24).

ניהול משק אנרגיה חכם

טכנולוגיית 5G תוכל לתמוך בתהליכי ניהול חכמים יותר של משק האנרגיה (חשמל, גז, מים) ולספק נתונים על צריכת האנרגיה בזמן האמת. היא תוכל לחבר בין ספקים לצרכנים באמצעות מערכות מדידה מתקדמות, ולהקים תחנות כוח וירטואליות[7] מוניציפליות ואזוריות (Federal Ministry of Transport and Digital Infrastructure, 2017, p. 11; Zaballos et al., 2020, p. 8). היא תוכל לתרום להפחתת עלויות השימוש באנרגיה, למשל באמצעות מעבר לתאורה ציבורית חכמה (שכבר קיימת בכמה ערים בעולם), לאפשר ניהול יעיל של משק החשמל ולאזן בין ביקושים גם בתקופות של צריכת שיא, ובכך לתרום לצמצום היקף השימוש בחשמל ולגרום להורדת המחירים (Prieger, 2020, p. 12). לבסוף, טכנולוגיית 5G תוכל לקדם את הטמעתם של שירותים חכמים במבנים ותשתיות, ואלה יאפשרו לנטר מערכות חימום, מים ואוורור ולשלוט בהן (Federal Ministry of Transport and Digital Infrastructure, 2017, pp. 11–12).

צמיחה כלכלית וצמצום פערים חברתיים

השימוש ב-4G הוגבל בעיקרו לטלפונים חכמים; לעומת זאת, טכנולוגיית 5G צפויה להשתלב באופן מלא בענף ההייטק במגוון תעשיות נוספות (Zaballos et al., 2020, p. 7). למהלך כזה צפויה להיות השפעה ישירה ועקיפה על הכלכלה ועל שוק העבודה העכשווי והעתידי בכמה היבטים, כפי שנפרט להלן (Duffy n.d., pp. 9–10):

תמיכה בשינויים ארגוניים: חיבור טוב יותר לרשת צפוי ליצור סביבות עבודה חדשות ולהגביר את שכיחותה של העבודה מהבית, ובכך לחסוך זמני נסיעה, להפחית עומסים בכבישים ולשפר את חיי הקהילה והמשפחה של העובדים (Dettling, 2017; Prieger, 2020, p. 9). טכנולוגיית 5G תאפשר לקיים עבודת צוות מרחוק באמצעות שידור וידאו באיכות גבוהה ושימוש בכלים של מציאות מדומה (VR) ורבודה (AR), כמו גם באמצעות 'אינטרנט המגע' (Tactile Internet) (Prieger, 2020, p. 10).

מקומות עבודה חדשים: אומנם עובדים רבים עלולים לאבד את מקום עבודתם נוכח השינויים הטכנולוגיים הצפויים, אך מנגד, הטמעת 5G צפויה לעודד פעילות כלכלית, ובאמצעות תמיכה בשינוי ובייעול מבנים ארגוניים – ליצור מודלים עסקיים, מוצרים, עסקים, ענפים ושירותים חדשים. השינויים שייווצרו עשויים להגביר את הביקוש לכוח עבודה חדש ומיומן וליצור מקומות עבודה חדשים במגזרים שונים (כהן, 2018, עמ' 2; Deloitte, 2019, pp. 49–50). טכנולוגיית 5G

7 תחנות כוח וירטואליות הן מערכות מבוססות תוכנה המסייעות לנהל, לאחסן ולקבץ אנרגיה המתקבלת מרשת מבוזרת של ספקי חשמל כגון חוות פאנלים סולאריים, תחנות רוח, תחנות הידרו חשמליות ועוד ובכך מסייעות בניהול חכם ובחיסכון באנרגיה.

עשויה, כאמור, להגדיל את שיעורי ההשתתפות של כוח עבודה חדש בשוק העבודה – בעיקר של עובדים מבוגרים ובעלי מוגבלויות ועובדים הנדרשים להעביר את עיקר זמנם בבית, כגון הורים לילדים קטנים (Dettling, 2017; Prieger, 2020, p. 9).

גידול בצמיחה כלכלית, בתל"ג ובתל"ג לנפש: בשעה שמדינות העולם – ובהן ישראל – סובלות מהתכווצות של כלכלותיהן עקב משבר הקורונה (הלפרן, 2020), השימוש בטכנולוגיות שמסתייעות ברשתות 5G, כמו מכשירי ה-IoT וטכנולוגיות ענן, הופך לחיוני בשל הפוטנציאל שלו לתרום לגידול בצמיחה הכלכלית, בתל"ג ובתל"ג לנפש[8] ולשיפור במדדים סוציו-אקונומיים נוספים.[9] הצפי לגידול זה מתכתב עם הצפי לגידול בשיעורי התעסוקה, פריון[10] העובדים ורווחי העסקים. נוסף על כך יתרום השימוש בטכנולוגיות המתקדמות להעצמת תהליכי חדשנות, יחזק את הקשר בין צרכנים לעסקים, ירחיב את הייצוא וישפר את תחרותיות הכלכלה בשוק הגלובלי (כהן, 2018, עמ' 2; Deloitte, 2019, pp. 49–50; Gruber et al., 2011).

עסקים, מסחר ופיננסים: 5G תאפשר לשדרג את ענף המסחר, הקמעונאות והפיננסים באופן שיחסוך זמן וכוח אדם וישפר את השירות ואת חוויית הלקוח (451 Research, n.d., pp. 3–4; Aria et al., 2020, p. 17; Duffy, n.d., pp. 9–10; Ericsson, 2018, p. 7). כבר כיום ניכרים גידול והאצה בהיקפי רכישות מוצרים ושירותים בטלפון החכם על פני רכישות באמצעות המחשב (m-commerce vs e-commerce). פריסה והטמעה של הטכנולוגיה תאפשר להקים ולהשתמש במחסנים אוטומטיים ולנהל מלאים באופן יעיל, לרכוש מוצרים במהירות מכל מקום – בהתבסס על שידורי וידאו חיים, הולוגרמות, שיחות באיכות 3D ועל כלים של מציאות רבודה ומדומה ולהפיג חששות מרכישה ברשת וחוסר ודאות בקרב לקוחות. הטכנולוגיה תאפשר ליצור בנקאים וירטואליים ולהתאים אישית את שירות הלקוחות מרחוק בענף המסחר והבנקים – לרבות שימוש ברובוטים ובחתימת זיהוי פנים באיכות גבוהה, ותסייע לקיים פגישות מאובטחות ממרחק עם יועצים פיננסיים.

תמיכה בתהליכי הכללה חברתיים (Inclusion) – פריסה והטמעה נרחבות של רשתות 5G בישראל עשויה לסייע בצמצום פערים בחברה הישראלית. הרחבת החיבור לרשת וכן חיבור לרשתות ה-5G גם באזורים מרוחקים בעלי חיבוריות מוגבלת יוכלו לסייע בהנגשתם של שירותים מרחוק ולצמצם פערים בין המרכז לפריפריה בתחומי הבריאות, החינוך, השירותים הממשלתיים והתחבורה ציבורית. ברמה הלאומית, הגדלת נפח הפעילות הכלכלית בעקבות אימוץ 5G עשויה להגדיל את הכנסות המדינה ולאפשר לה להשקיע בטווח הארוך משאבים רבים יותר בשירותים ציבוריים חברתיים-כלכליים (Deloitte, 2019, pp. 49–50).

8 תוצר לאומי גולמי ותוצר לנפש משמשים מדדים מרכזיים לעוצמתן הלאומית של מדינות (Gat, 2006, p. 516).

9 לפי מחקרים שבחנו זאת אמפירית: Deloitte, 2019; Oxford Economics, 2019; The App Association [ACT], 2019 ועוד. עם זאת, ראוי לסייג את הדברים; ייתכן שהקשר הפוך דווקא – גידול בתל"ג של מדינות מגביר את הביקוש לשימוש ברשתות סלולריות מתקדמות.

10 זרימה מהירה ואיכותית של מידע באמצעות רשת אלחוטית מאפשרת להגביר עד מאוד את היעילות. מחקרים שנערכו הצביעו על העלאה ניכרת בפריון של חברות, על חיסכון בזמן ועל הגברת היעילות בעבודה בעקבות אימוץ 4G, ולכן ההשערה היא ש-5G תגביר מגמה זו (Deloitte, 2019, p. 49). מחקרים אמפיריים שנערכו בחנו את הקשר בין מהירות ההורדה כמשתנה פרוקסי (proxy variable) למדידת איכות החיבוריות ובין משתנה התל"ג. למשל, במחקר שנערך ב-35 מדינות בשנים 2002–2016 נמצא שעלייה במהירות ההורדה נקשרה לעלייה של 0.9% בתל"ג.

רפואה

למרות חסרונותיה ומגבלותיה, מערכת הבריאות של ישראל נחשבת למצוינת ואיכותית (ויסברג, 2018). פריסה והטמעה של רשתות 5G יאפשרו לישראל להמשיך לשמר את מעמדה כמדינה מובילה בתחום הרפואה והבריאות בעולם, כל עוד מקבלי ההחלטות ישכילו לשלב בין הידע, המדע והטכנולוגיה המתקדמת בכלל, ובתחום הרפואה בפרט, לבין ההון האנושי (קריסטל, 2019). על יסוד האמור בספרות המחקר, ההערכה היא שרשתות ה-5G יאפשרו לשפר את עבודת מערכות הבריאות והצוותים הרפואיים ובייחוד את איכות השירות והטיפול. להלן יובאו בפירוט שש השפעות עיקריות שעשויות להיות לפריסת הטכנולוגיה המתקדמת ולהטמעתה על תחום הרפואה:

(1) היכולת להעביר במהירות ובמהימנות קובצי נתונים גדולים במיוחד, כגון תצלומים רפואיים וסריקות (תצלומי MRI למשל), צפויה לזרז ולייעל את המערכת ואת מתן הטיפול.

(2) זמן ההמתנה הקצר בהעברת הנתונים יקל להגדיל את שוק שירותי הרפואה מרחוק (טלרפואה). שירותים אלה עתידים לסייע בפתרון בעיית המרחק הפיזי בין רופאים למטופלים המתגוררים באזורים מרוחקים ממרכזים רפואיים, ולייעל במידה רבה את מתן השירותים הרפואיים (AT&T Business, n.d.). נוסף על כך, רשתות 5G יאפשרו להפעיל מרחוק רובוטים, וכך יאפשרו למומחים ולמנתחים להשתתף בניתוחים מסובכים במדינות אחרות (Whittle, 2019). הצורך בטיפול ובמעקב רפואי מרחוק שרשתות ה-5G יכולות לספק מקבל משנה תוקף בעת התפרצות מגפות, כדוגמת הקורונה (KPMG, 2020, p. 9).

(3) היקף העברת הנתונים יאפשר לערוך הדמיות של תרחישים רפואיים מורכבים, לספק לחולים במצב קשה טיפולים חלופיים ולהפחית כאב ולחץ. הנגשת תוכן מרגיע באמצעות כלים של מציאות מדומה ורבודה תאפשר להעניק טיפולים רפואיים חדשניים, פולשניים פחות וממרחק.

(4) שימוש ברשתות 5G יאפשר להקנות לצוותי רפואה יכולת לעקוב ממרחק אחר מצבם של מטופלים ולקבל מידע עדכני ועכשווי עליהם, לשם שיפור השירות והתאמת טיפול מונע אישי.

(5) המעבר לרשתות 5G יאפשר לצוותים רפואיים להסתייע בטכנולוגיות חדשות (כגון בינה מלאכותית) כדי לאבחן בעיות רפואיות ולבחור את תכנית הטיפול המתאימה עבור חולה מסוים, וכן לבחור את שלב ההתערבות המתאים ולנבא סיבוכים אפשריים הכרוכים בטיפול (AT&T Business, n.d.).

(6) פריסתן והטמעתן של רשתות 5G תשפר את היכולת לנהל מצבי חירום אזרחיים בהיקפים נרחבים בזמן התרחשותם. טכנולוגיה זו תאפשר העברת נתונים באמצעות קטעי וידאו מרכבי חירום ואמבולנסים חכמים המפנים פצועים, כדי להכין עבורם בבית החולים טיפול מתאים מראש. כמו כן, היא תשפר במידה ניכרת את המוּדָעוּת המצבית ואת מתן התמונה המלאה במצבי חירום באמצעות צילומים שאיכותם גבוהה בזמן אמת ונתונים ממצלמות ומחיישנים המותקנים על רחפנים; אלו יסייעו גם בהעברת סיוע רפואי לאזורי אסון שהגישה אליהם נחסמה (Whittle, 2019).

חינוך

במדינה המקדשת את ערכי הלמידה, ההשכלה הגבוהה והמצוינות המדעית, מערכת החינוך היא משאב אסטרטגי חיוני, אשר לא רק משפיע על יכולתה של ישראל לשמר את יתרונותיה היחסיים, אלא במידה רבה קובע את עתידה וקיומה (חזן, 2014). אולם נראה כי מערכת החינוך הישראלית מתקשה להסתגל לקצב השינויים המהיר ולהכין את דור העתיד להתמודדות עם אתגריו (איזנברג וזליבנסקי, 2019, עמ' 9, 13). התאמת מערכת החינוך לעידן הנוכחי תדרוש לזנוח את ההתמקדות בידע מבוסס זיכרון וחֶלֶף זאת להתמקד בפיתוח כישורים של חשיבה ביקורתית, יצירתיות וחדשנות, פתרון בעיות, עבודת צוות, תקשורת, ניהול מידע, הכוונה עצמית, למידה לאורך החיים ועוד (איזנברג וזליבנסקי, 2019, עמ' 13).

נגישות טכנולוגית צפויה בשנים הקרובות להרחיב את הגישה למשאבים דיגיטליים מעשירים המאפשרים לרכוש מיומנויות וידע מגוונים. מודל הלמידה העתידי צפוי להתאפיין בסביבה מיידית, וירטואלית ואינטראקטיבית שתאפשר לתלמידים ללמוד ולתקשר בדרכים שונות מאלו המוכרות לנו כיום. המודל יתאפיין בלמידה גמישה ואיכותית המתמקדת בלומד עצמו, מותאמת לו אישית ומכוונת לרכישת מיומנויות ולפיתוח יכולת למידה שיתופית. טכנולוגיית 5G תנגיש הזדמנויות בחינוך ותאפשר להשתתף במגוון נרחב של קורסים מקוונים (Aria et al., 2020, p. 18). היא תאפשר לשלב בתהליך הלמידה כלים מתקדמים שיתמכו במודל זה, כגון אמצעי מציאות מדומה ורבודה, אינטרנט מגע, מערכות לניתוח הרגלי למידה ולשיפורם המותאמות באופן אישי לתלמיד, כיתות דיגיטליות, קמפוסים חכמים, רובוטים המחוברים לסביבת ענן שיסייעו לתלמידים עם צרכים מיוחדים ואמצעים שיאפשרו למורים להתמקד בתהליך הלימוד במקום בתהליכים מנהלתיים (Jamshidi, n.d.; Mirzamany & Neal, n.d.).

נראה אם כן, שפריסתה והטמעתה של טכנולוגיית 5G יאפשרו לשפר את חוויית הלמידה ויתמכו במאמצי מערכת החינוך להכשיר את תלמידי ישראל לקראת אתגרי המאה העשרים ואחת. החשיבות בהטמעתן התחדדה במיוחד נוכח משבר הקורונה, שאילץ את מערכת החינוך והאוניברסיטאות בארץ ובעולם לבצע מעבר ללמידה מלאה או היברידית מרחוק.

מעמד אזורי ובין-לאומי

עם התפרקות ברית המועצות והמעבר לעולם של הגמוניה אמריקאית, גברה בחקר היחסים הבין-לאומיים הפופולריות של המושג 'עוצמה רכה' (Soft Power), מושג שטבע פרופסור ג'וזף ניי מאוניברסיטת הרווארד. עוצמה רכה מיוחסת ליכולתן של מדינות, כחלק מעוצמתן הלאומית, להשתמש באמצעים בלתי כוחניים כמו תרבות, ערכים וחינוך, וכן מוסדות ממשל וכלכלה אטרקטיביים, המשמשים מקורות ליצירת השפעה ושיתופי פעולה בעולם. לעומת זאת, הפעלה מסורתית של משאבי עוצמה לאומית, היינו שימוש של מדינות בכוח צבאי או כלכלי, הם אמצעי 'עוצמה קשה' (Hard Power), שנועדו לאכוף את רצונן על מדינות ושחקנים אחרים בפוליטיקה העולמית (Nye, 2004).

בתחילת הדרך יוחסה העוצמה הרכה בעיקר לארצות הברית, אולם לאחרונה התקבע שגם מדינות קטנות יכולות להפעיל עוצמה רכה כלפי חוץ, כדי להגביר את כוחן בפוליטיקה העולמית

ללא תלות במידותיהן (Nye, 2019). מדינות קטנות, דוגמת סינגפור, פינלנד, אסטוניה ואחרות, זכו למעמד בעולם באמצעות מיתוג והשקעה בכלכלותיהן המתקדמות והטכנולוגיות ובמערכות רווחה, ממשל וחינוך מצטיינות; כל אלה אפשרו להן להעצים את תדמיתן ואת יוקרתן הבין-לאומית, לקדם שיתופי פעולה ולהרחיב את מעגל הבריתות שלהן (Chong, 2010; Karabeshkin & Rusetski, 2013, pp. 46–47).

כמדינה קטנה במונחי שטח וכלכלה, משאבים וכוח אדם, המאוימת תכופות ותלויה בסביבה החיצונית לקיומה, הצטיינותה של ישראל בתחום הטכנולוגיה והחדשנות מבליטה את יתרונותיה היחסיים במונחים בין-לאומיים. מעמדה זה של ישראל תורם לשיפור המוניטין והתדמית שלה ולהקרנת עוצמתה הרכה במונחים אזוריים וגלובליים. לצד שיפור תדמיתה ומעמדה הבין-לאומי, יכולת החדשנות מאפשרת לישראל גם להעמיק קשרים עם מדינות וליצור לעצמה קשרים חדשים עם מדינות – גם כאלה שאינן מקיימות עימה יחסים דיפלומטיים רשמיים.[11] אימוץ טכנולוגיות מתקדמות, ובהן רשתות 5G, עשוי לתמוך במאמציה של ישראל להמשיך ולשמש מרכז עסקי דינמי, תוסס, יזמי ואטרקטיבי, וכך לאפשר לה להמשיך לעמוד בחזית החדשנות הטכנולוגית העולמית, למשוך אליה השקעות כלכליות זרות נוספות ולקדם שיתופי פעולה בילטרליים ומולטילטרליים כאחד (Press Trust of India, 2020; Osher & Ivri, 2019).[12]

איומים בתחום אבטחת הסייבר – מבט על

בעת כתיבת שורות אלו רשתות 5G טרם נכנסו לשימוש מסחרי נרחב, ולכן גם מפת האיומים עליהן מבוססת בחלקה על הערכות בדבר שימושים עתידיים בהן. איומי סייבר על רשתות 5G עלולים להוביל לשיבושי השירותים המתבססים על הרשתות, לריגול וגנבת מידע, לשינוי ומניפולציה על מידע העובר ברשתות ולפגיעה בתשתיות דיגיטליות המסתמכות על הרשתות. האימוץ וההטמעה של רשתות 5G מתרחשים על רקע מפת איומים סבוכה המתאפיינת בריבוי מתקפות סייבר על שרשראות אספקה; איומים אלו קיימים אומנם גם בהקשר של רשתות תקשורת מדורות קודמים, אולם ההסתמכות על רשתות 5G – שתלך ותגבר בעתיד – צפויה להגביר עד מאוד את עוצמת האיום. ענפי תעשייה ותשתיות רבים צפויים להסתמך על רשתות 5G, והיכולת להעביר נתונים רבים צפויה לאפשר שימוש בטכנולוגיות כגון ערים חכמות ורכבים אוטונומיים, בינה מלאכותית ומכשירי IoT. רשתות 5G עתידות להפוך לתשתית שבאמצעותה יתקשרו מכשירים רפואיים, מערכות לניתוב ולניהול תחבורה, מערכות נשק, תשתיות אנרגיה ומערכות לבקרה תעשייתית. משכך, חשיבות אבטחת הסייבר של רשתות 5G אינה נובעת רק מחולשות החושפות אותן לאיומי סייבר, אלא גם מהחיוניות הגוברת שלהן ומן הנזק הצפוי לחיי היום-יום, לכלכלה, לרכוש, לנפש ולביטחון הלאומי עקב פגיעה בהן (Wheeler & Simpson, 2019).

11 ראו את תהליכי הנורמליזציה עם איחוד האמירויות ועם בחריין.

12 ב"הסכמי אברהם" בין מדינת ישראל לאיחוד האמירויות הוסכם כי יוקמו "מסגרות לפיתוח חדשנות בתחומי טכנולוגיות מידע ותקשורת", ובפרט רשתות 5G, ערים חכמות ומתן שירותים (Abraham Accords Peace Agreement, 2020). ארצות הברית, הודו וישראל משתפות פעולה בתחום אבטחת רשתות 5G ובכלל, כחלק משאיפתן לנסות להתמודד עם "אתגרים באזורים מתפתחים בעולם, ולהפוך לכוחות מובילים ומנהיגים במרחב הדיגיטלי" (PTI, 2020). חברות תקשורת מערביות כמו נוקיה, אריקסון וטי-מובייל מתעניינות בשוק הישראלי מתחילת תהליכי פריסתן של רשתות 5G (Osher & Ivri, 2019).

מסמך זה אינו דן בחולשות אבטחה ספציפיות בציוד חומרה, בפרוטוקולים ובתוכנות המרכיבות את רשתות 5G, שכן חולשות אבטחה קיימות בכל תוכנה וחומרה ואינן ייחודיות לרשתות אלה (Sullivan & Lucas, 2020). נוסף על כך, מכיוון שטכנולוגיית 5G מצויה עדיין בשלבי ניסוי, ותקנים חדשים מתפרסמים באופן תקופתי, אפשר להעריך כי יימצאו חולשות חדשות ואילו חולשות ופערים ישנים יתוקנו.

להלן יפורטו האיומים המרכזיים על רשתות 5G.

'ירושת' חולשות ישנות: בשלב הראשון צפויות רשתות 5G להסתמך באופן חלקי על תשתיות של רשתות 4G (Non-Standalone), ובשל כך הן יהיו חשופות לחולשות אבטחה שמקורן ברשתות אלה. חולשות אלו עלולות לאפשר לתוקף לאתר מיקום של משתמשים, להוציא לפועל מתקפות למניעת שירות (DoS) ועוד (Ekström, 2019). דוגמאות לאיומי סייבר שמקורם ברשתות 4G הן מתקפת ToRPEDO, המאפשרת לקבוע את מיקומו של מכשיר המשתמש, ומתקפת Piercer, המאפשרת לזהות את מספר הזיהוי הייחודי המאוחסן בכרטיסי הסים של המשתמש (IMSI)[13] ולקבל גישה לשיחות ולהודעות שלו (Hussain et al., 2019).

בשלב זה תימשך ההסתמכות על פרוטוקול GTP[14] - חלק מקבוצת פרוטוקולים לתקשורת מבוססת IP, המשמשים בין השאר להעברת מידע של משתמשים בין רשת הליבה לרשת הגישה לרדיו (RAN)[15] ובין רשתות אלחוטיות. פרוטוקול GTP משמש את רשתות 2G, 3G ו-4G ומאפשר מעבר לרשת מתקדמת פחות במקרים שבהם האותות חלשים. אחת החולשות הידועות של פרוטוקול זה היא שהוא אינו בודק את מיקום המשתמש, ובכך מקשה לזהות תעבורה בלתי לגיטימית מטעם תוקפים. חולשה בסיסית זו עלולה לאפשר מתקפות DoS על ציוד של מפעילת הרשת ולפגוע בהתקשרותם של משתמשים רבים אליה; איומים נוספים הם התחזות למשתמש, גנבת פרטי הרשאות ועוד. ההסתמכות הראשונית של רשתות 5G על רשתות 4G צפויה לחשוף גם אותן לאיומים שמקורן בחולשות פרוטוקול GTP (Positive Technologies ,2020).

לאחר אימוץ רשתות 5G צפויות עלויות התיקון של חולשות בפרוטוקולים ובארכיטקטורות של רשתות 4G לצמוח ולהקשות על חברות התקשורת (Asokan, 2020). על כן גוברת החשיבות לתקן חולשות אבטחה ישנות ברשתות מדורות קודמים בטרם אימוץ רשתות 5G. עם הטמעת רשתות 5G בתצורת Non-Standalone כדאי ליצור סביבה מנוטרת ומאובטחת בנקודת החיבור שבינן לבין הרשתות מהדורות הקודמים.

הסתמכות רבה על תוכנות: רשתות 5G צפויות להסתמך באופן נרחב על תוכנות, ובכך הן עלולות להיחשף לחולשות הנובעות מכשלים בתהליכי פיתוח התוכנות בידי היצרנים או מהגדרות תצורה. גם פונקציות המשמשות גורמי ביטחון ואכיפה לצורכי יירוט מידע החיוני לסיכול פיגועים, מאבק בפשיעה וחקירות צפויות להיות מבוססות על תוכנה ועל כן חשופות לאיומי סייבר פוטנציאליים ולניצול מצד גורמים זדוניים (NIS Cooperation Group, 2019, pp. 19–20).

שרשראות אספקה מורכבות: כדי לתת מענה למספר הולך וגובר של מכשירים שיחוברו לרשת ולאפשר העברת נתונים רבים וזמן המתנה קצר, רשתות 5G עושות שימוש בתחום תדרים רחב הרבה יותר (עד 100 גיגה-הרץ), שנכללים בו גלים מילימטריים. בשל אורכם הקצר, גלים

13 International Mobile Subscriber Identity; ה-IMSI מאפשר למשתמש להזדהות בפני הרשת.

14 GPRS (General Packet Radio Service) Tunneling Protocol.

15 Radio Access Network.

מילימטריים מתקשים לעבור דרך מכשולים כגון בניינים וצמחייה, ועוצמתם תלויה במזג האוויר ועלולה להיפגע כתוצאה ממשקעים. כדי לשפר את יכולת הכיסוי שלהן, נכללת בארכיטקטורה של רשתות 5G פריסה רחבה של אתרים סלולריים קטנים (small cells), שציוד הרדיו שלהם מאפשר שידור לטווח קצר בפסי תדרים גבוהים; אתרים אלה משלימים את התרנים הסלולריים (macro cells) המספקים כיסוי רחב יותר (Gunnerson & Reall, n.d.).

אם כן, הארכיטקטורה של רשתות 5G מורכבת ומבוזרת הרבה יותר מזו של הדורות שקדמו לה. עם הגידול במספר הרכיבים ובסוג הרכיבים הנדרשים להרכבת התשתית של רשתות 5G גדלות גם שרשראות האספקה שלהן ביחס לרשתות מדורות קודמים. מצב זה מחייב לתת את הדעת על אבטחת הסייבר של שרשראות האספקה, לבחון את תהליכי ניהול הסיכונים בקרב הספקים, לצמצם את התלות בספקים בודדים ועוד (NIS Cooperation Group, 2019). דוגמה לסיכונים שבשרשראות האספקה היא אזהרות שהשמיעו בכירים בארצות הברית בפברואר 2020 כי חברת התקשורת הסינית Huawei התקינה בתחנות בסיס ובמתגים מתוצרתה 'דלתות אחוריות', וכך שימרה את גישתה לרשתות סלולריות (Hamilton, 2020).

בהסתמכות על ספקים רבים של חומרה ותוכנות יש גם מן היתרון, משום שהיא מאפשרת למזער את ההסתמכות על ספק אחד, וכך לאפשר שרידות והמשך מתן שירות גם בעת שיבושים או במקרים של מתקפות סייבר על תוכנה או חומרה של אחד מהספקים (Sullivan & Lucas, 2020). עם זאת, יצרנים, ספקים וספקי משנה עלולים להיות ממוקמים במדינות שונות, ומצב זה עלול להקשות מאוד לפקח על תהליכי בקרת האיכות שלהם.

הגדלת שטח פני התקיפה וחשיפת הרשת לאיומים נרחבים: יכולת העברת הנתונים של רשתות 5G צפויה לתמוך בחיבורם של מיליוני מכשירי IoT ובהם חיישנים, מצלמות, מכשירים רפואיים ומכשירים ביתיים המחוברים לרשת, יישומים צבאיים (Internet of Military Things) ויישומים תעשייתיים (Industrial Internet of Things). בשנים האחרונות הושמעו אזהרות רבות בנושא רמת האבטחה הנמוכה של מכשירי IoT – הנובעת ממחסור בתקני אבטחה ומתמריצי השוק, המעודדים את היצרנים להוציא לשוק מכשירי IoT במהירות וללא מנגנוני אבטחה (Bieler, 2019; UK Department for Digital, Culture, Media & Sport, 2018, pp. 7–8). הגידול הנחזה בשימוש במכשירי IoT – כ-75 מיליארד מכשירים ברחבי העולם ב-2025 – יגדיל את שטח פני התקיפה (attack surface) ויסייע להפוך את רשתות 5G למטרה מרכזית עבור גורמים זדוניים (Haddix, 2019).

איומי סייבר על תשתיות ומרכיבים מסוימים של רשתות 5G

לצד איומים על רשתות 5G הנובעים ממאפייניהן הכלליים, מוכרים גם איומי סייבר על מרכיביהן המסוימים של הרשתות, ובהם מרכיבי רשת הליבה ורשת הגישה לרדיו (RAN).

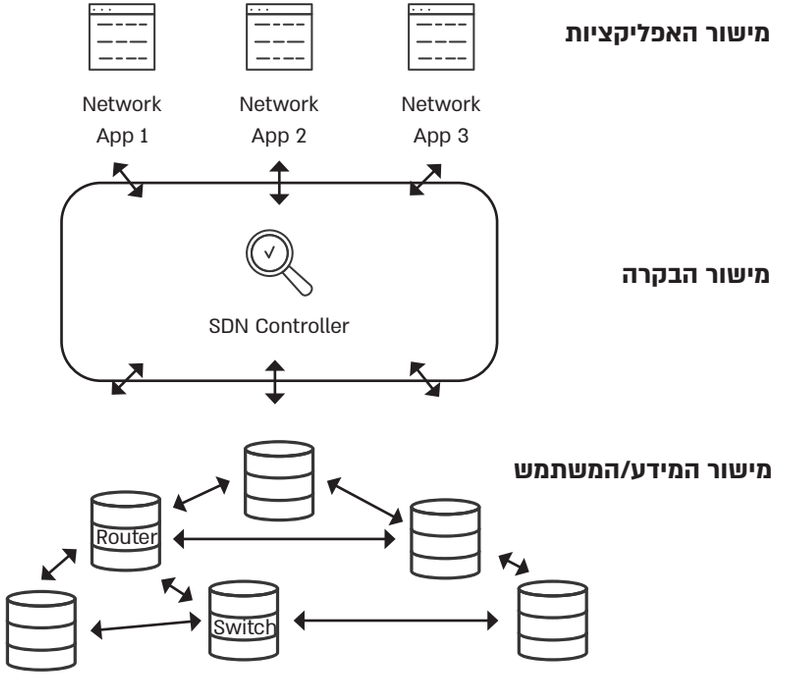
איומי סייבר על רשת הליבה

השינויים ברשת הליבה בעקבות אימוצה של טכנולוגיית 5G עתידים להוביל לאימוץ גישות חדשות לארכיטקטורת רשת, כגון **מעבר לשימוש בתוכנות** (softwarization) **ווירטואליזציה.** המעבר לשימוש בתוכנות פירושו כי שינויי תצורה ברשת ועדכונים שלה אינם מצריכים החלפת רכיבי חומרה ספציפיים, ובכך נחסכים זמן וכסף. המרכיב המרכזי של מעבר זה הוא הסתמכות

רבה על גישת **רשת מוגדרת-תוכנה** (SDN)[16] – גישה חדשנית לניהול רשת המאפשרת ניהול גמיש וריכוזי שלה, מאפשרת למפעיליה לעדכן ולשנות את תצורתה בהתאם לשינויים ולשירותים שעליה לספק ועוד.

ברשתות מדורות קודמים, בכל מתג ונתב הייתה פונקצייה של בקרה ושליטה על המידע – לניהול הרשת, ליישום פרוטוקולים, לניתוב המידע למסלול מסוים ולאבטחה. לעומת זאת, גישת SDN מפצלת את פונקציות העברת חבילות המידע (packet forwarding) ואת פונקציות הניהול והשליטה ברשת לשני מישורים: מישור הבקרה (Control Plane) ומישור המידע או המשתמש (Data/User Plane) (ראו תרשים א').

תרשים א': החלוקה למישור האפליקציות, המידע/המשתמש ולמישור בקרה בארכיטקטורת SDN



על אף היתרונות שבחלוקה זו, לא מן הנמנע כי גורמים זדוניים ימצאו דרך לפרוץ לאחד ממרכיבי מישור המידע או מישור הבקרה כדי לזייף בקשות מידע העוברות בין הבקרים במישור הבקרה וכך להשפיע על תהליכי התצורה והניהול של הרשת. כמו כן, ההפרדה בין מישור הבקרה למישור המידע באמצעות ממשקים מגבירה את הסיכון שתוקף פוטנציאלי יוכל לשבש את מעבר המידע בין המישורים השונים (Martin et al., 2015, pp. 20–21).

את איומי הסייבר על ארכיטקטורת SDN אפשר לחלק על פי המישורים השונים.

איומי סייבר על מישור האפליקציות: בתרחיש מסוג זה יכול תוקף לקבל גישה בלתי מאושרת

16 Software-Defined Network.

או הרשאות גישה לאחת מהאפליקציות ולנצלן כדי להעמיק את חדירתו לרשת, להיחשף למידע המועבר בין הבקרים במישור הבקרה, לחסום אותו ועוד (Martin et al., 2015, pp. 20–21).

איומי סייבר על מישור הבקרה: הבקר מתפקד כמערכת ההפעלה של הרשת, ועלול לשמש מטרה מרכזית עבור גורמים זדוניים. מקורם של רוב איומי הסייבר על מישור הבקרה הוא בחולשות תוכנה של האפליקציות או בחולשות תוכנה או חומרה במישור המידע, בתשתיות הרשת. כבר ב-2015 הצליחו חוקרים מגרמניה לפתח אפליקציה זדונית המכילה נוזקה מסוג Rootkit, המסוגלת לשכתב את פקודות הניתוב של הבקר ולשנות את כל ניתוב המידע. החוקרים הזהירו כי תוקפים עלולים להפיץ עדכוני תוכנה מזויפים לאפליקציות או לפרוץ לחנות אפליקציות SDN במטרה להפיץ נוזקות (Röpke & Holz, 2015). כמו כן יכול התוקף להתחזות לבקר, לזייף פקודות העוברות מהאפליקציות לבקר או מהבקר למתגים, לעקוף את מדיניות האבטחה ולשלוט בניתוב המידע ברשת (Hogg, 2014).

איומי סייבר על מישור המידע: גם במישור המידע יכול תוקף לנצל חולשות בתשתיות חומרה (כגון מתגים ונתבים) כדי לפרוץ אליהם ולשלוח חבילות מידע לבקר באופן שיגרום לעומס ולמניעת שירות (DoS). כמו כן יכול תוקף לנצל חולשות בפרוטוקול OpenFlow, המשמש לתקשורת בין רכיבי הרשת לבין הבקר, כדי לשנות את רשומות טבלת הניתוב באופן שיפגע בתפקוד הרשת (Shaghaghi et al., 2020). איום נוסף הוא יירוט מידע העובר בין מרכיבי חומרת הרשת ובין החומרה לבקר (Lourenço & Marinos, 2019, pp. 58–59).

הוירטואליזציה של פעילות רשת הליבה[17] מאפשרת לייצר פלטפורמות חומרה, מערכות הפעלה ומכשירים וירטואליים ולהעביר את פעילות הרשת למרכזי נתונים ולענן. השימוש בתוכנה במקום חומרה מאפשר גמישות רבה יותר, מגביר את מהירות העברת המידע ומקצר את זמן ההמתנה באמצעות הצבת צומתי רשת (network node) וירטואליים בקרבת המשתמשים – במקום צומתי רשת פיזיים, שכאשר הם מוצבים במרחק ניכר מן המשתמשים נפגעת מהירות העברת המידע (Condoluci & Mahmoodi, 2018). עם זאת, גם במצב של וירטואליזציה יכול תוקף לפרוץ לתשתיות פיזיות המפעילות את הפלטפורמות הוירטואליות, כגון שרתים ומרכזי נתונים (Martin et al., 2015, p. 23). כמו כן, אפשרית גם תקיפת המערכת הוירטואלית עצמה, כמו מתקפת virtual machine escape – פריצה למכשיר או למערכת הוירטואלית, שאמורה להיות מבודדת לחלוטין ממערכת ההפעלה המריצה אותה, ומשם לשכבת הניהול של המערכת הוירטואלית (Hypervisor). משם יכול תוקף לפרוץ למערכת ההפעלה ולשלוט בכל המערכות והמכשירים הוירטואליים (Lal, Taleb, & Dutta, 2017). איומים אלו מחייבים ניטור ומעקב מתמידים שיאפשרו לזהות במהירות פריצה למערכת וירטואלית, להשבית אותה וליצור מערכת חלופית להמשך תפקוד תקין.

רוב איומי הסייבר על המישורים השונים אינם חדשים או ייחודים לרשתות 5G; אולם על אף יתרונותיה הרבים, החלוקה וההפרדה בין המישורים אינה נותנת מענה לאיומי הסייבר, ואילו ריכוז השליטה ברכיבי חומרת הרשת אצל הבקר עלול לאפשר לתוקף המשתלט עליו לשלוט בכמה רכיבי חומרה.

17 NFV – Network Function Virtualization.

איומי סייבר על רכיבי הרשת שאינם ליבה – רשת RAN

רשת הגישה לרדיו (RAN) היא מקטע הנפרד מרשת הליבה, אשר מקשר בין רשת הליבה למכשירי המשתמשים. הרשת מורכבת מתחנות בסיס שיש בהן אנטנות ומְבַקר השולט בתחנות הבסיס.[18] היא אחראית לקיום תקשורת רדיו בין תחנות הבסיס למכשירי המשתמשים ומעבירה אליהם את תעבורת המידע מרשת הליבה.

רשת הליבה אחראית להצפנת המידע, ואילו רשת הגישה לרדיו אחראית רק להעברתו. הפרדת הרשתות זו מזו וחלוקת התפקידים ביניהן הובילה לאימוץ תפיסה המייחסת חשיבות פחותה לאבטחת הסייבר של מרכיבי RAN, שכן אמינותו וסודיותו של המידע (העובדה שהמידע לא עבר שינויים בדרך ושאיש מלבד הצדדים המתקשרים לא נחשף אליו) נבדקות ברמת רשת הליבה (Kennedy, 2019, p. 4).

עם זאת, בעת פריסתן הראשונית של רשתות 5G (בתצורת Non-standalone) יחוברו תחנות הבסיס החדשות (gNB) לתחנות בסיס של רשתות 4G קיימות (eNG), ומשם יועבר המידע לרשת הליבה של רשת 4G. מידע של משתמשים צפוי להישלח כשהוא מוצפן, אולם עם הגעתו לתחנת הבסיס של רשת 4G הוא יפוענח לקראת הצפנה נוספת והעברה לרשת הליבה; שלב פענוח המידע בדרכו אל היעד יוצר פרצת אבטחה המאפשרת לתוקף ליירט מידע של משתמשים (Teppo & Norrman, 2020).

כיום פועלים ארגוני תקנים לנסח תקנים שיגדירו את החובה להצפין – בטרם יישלחו לרשת – את פרטי הזדהות המשתמש בפני הרשת, המאוחסנים בכרטיס הסים של המשתמש (IMSI). אולם בכנס Black Hat 2019 הדגימו חוקרים כי פרטיותם של משתמשים ברשתות 5G חשופה עדיין לאיומי סייבר בדמות יירוט פרטי IMSI, למשל בדרך של התחזות לתורן סלולרי באמצעות מכשירים כגון מכשיר Stingray (Newman, 2019). איום ההתחזות לתחנות בסיס לגיטימיות עלול לאפשר לתוקף לקבל לידיו מידע השייך למשתמשים, לעקוב אחר משתמשים או להוציא לפועל מתקפת DoS על שירותי הרשת (5G Americas, 2018). על אף המאמץ לנסח תקנים עבור פרוטוקולים לאימות הדדי בין המכשירים לבין הרשת, גם גורמים זדוניים צפויים להמשיך לפתח את יכולותיהם לגנוב מידע ולחבל בפעילות רשתות 5G (Nakarmi, 2018).

איומים נוספים, המוכרים מהשימוש בתדרי רדיו, הם איומי שיבוש אותות (jamming) – שידור אותות בתדרים זהים לתדרי רשת הגישה לרדיו במטרה "לדרוס" אותם, וזיוף אותות (spoofing). השימוש בתדרים מילימטריים ברשתות 5G מקנה אומנם חסינות מסוימת ומקשה על שיבוש התדרים, אולם רשתות 5G יכללו עדיין שימוש נרחב בתדרי רדיו שמתחת לתדרים המילימטריים, תדרים שאותם קל יותר לשבש (Lichtman et al., 2018).

רשתות 5G – יתרונות אבטחה בספק

לצד האיומים והחסרונות צפויים מרכיבים ותכונות שונות של רשתות 5G לתרום לשיפור אבטחת הסייבר של הרשתות הסלולריות והמידע העובר בהן. השימוש בבקרי רשת מבוססי תוכנה המרכזים את ניהול הרשת תוך צמצום התלות בחומרה פיזית, צפויים להקנות לארכיטקטורת הרשת

18 RNC – RAN Controller.

גמישות ולאפשר למנהלי הרשת לנטר ולנהל את הרשת, לעדכן ולשנות תצורה והגדרות באופן ריכוזי (Wang, 2016). וירטואליזציית הרשת תאפשר לפצל רשתות (network segmentation), להעביר אפליקציות ונתונים רבים לענן באופן שיפחית את הסיכון שבהשבתה או בנזק לתשתיות חומרה וכן להקים מכונות וירטואליות לטובת גיבוי במקרה של תקלות (Marinho, 2019).

לרשתות 5G פוטנציאל לכלול תיקונים לחולשות אבטחה מרשתות קודמות ואף חידושים ומאפיינים שיגבירו את אבטחת הסייבר של המידע והשירותים המשתמשים בהן. עם זאת, היישום של יתרונות האבטחה הרבים של 5G תלוי בתקנים וביישום נכון של מפעילות הרשת. מכיוון שהתקנים נקבעים על פי מדינות – בהן גם סין, הנאשמת בניסיון להפוך את תהליך התקנון לפוליטי (Williams, 2019) – יישומם הוא וולונטרי. בשל כך תמריצי שוק כגון מחיר, מהירות פיתוח והוצאה לשוק וביצועים גבוהים עלולים להוביל ליישום חלקי בלבד של התקנים על חשבון יתרונות אבטחת הסייבר הפוטנציאליים של הרשתות (Schneier, 2020).

אבטחת הסייבר של רשתות 5G – תובנות וצעדים למזעור הסיכונים

ההתמקדות הרבה במאבק המעצמות הגאו-טכנולוגי בין ארצות הברית לסין עלולה להוביל למחשבה שהסיכונים היחידים הנשקפים לרשתות 5G הם איומי הסייבר והריגול הנובעים מהשתתפות החברות הסיניות בפרויקט והאפשרות כי ישראל תפגע ביחסים ההדוקים עם ארצות הברית או ביחסי המסחר המתהדקים עם סין. עם זאת, חשוב לזכור כי התמקדות יתר בתחרות בין ארצות הברית לסין לא תמנע את חשיפת הרשתות לאיומי סייבר שעלולים לנבוע ממבנה לקוי, מקיומן של חולשות אבטחה או מניהול ותפעול לקויים של מפעילי הרשת.

בדומה לכל מערכת או טכנולוגיה, גם לרשתות 5G אי אפשר להעניק אבטחה מוחלטת. חולשות אבטחה, טעויות קוד, מבנה או ארכיטקטורה לקויים, אי-עמידה בתקנים או ברגולציה, ניהול ותפעול לקוי וכן פיתוח מתמיד של היכולות והמיומנויות של שחקנים זדוניים ושימור האינטרס שלהם להסתנן לרשת או לשבש פעילות של מערכות – כל אלה צפויים לאיים איום מתמשך על רשתות 5G. לפיכך, גישה נכונה לאבטחת הסייבר של הרשתות צריכה להתמקד בניהול הסיכונים – כלומר בצעדים שמטרתם למזער את האיומים ולהקשות על תוקפים פוטנציאליים. להלן יפורטו מגוון צעדים כאלה.

שמירה על חסינות הרשת: חסינות זו מתבססת על ההנחה שכל רכיב חומרה או תוכנה עלול להיות חשוף למתקפות סייבר. כדי להתמודד עם מצב כזה יש לשקול לפצל את הרשתות לרשתות משנה (segmentation) ולהשתמש ביתירות (redundancy). פיצול הרשתות ימנע מתוקפים לעבור בין החלקים השונים של הרשת או לכל הפחות יקשה עליהם לעשות זאת, ועשוי לעכב את התוקפים באופן שיאפשר את גילוים. יתירות תבטיח כי אף אחת מן הפונקציות של הרשתות לא תתבסס על רכיב יחיד, וכי רכיבי גיבוי יבטיחו את פעילותן גם במקרה של כשל או שיבוש (Sullivan & Lucas, 2020). אומנם עקרון היתירות בא לידי ביטוי גם בהסתמכות על כמה יצרני ציוד ורכיבים, אולם בתחום טכנולוגיית 5G מספר היצרנים המספקים גם ציוד לרשת RAN קטן מאוד;[19] כמו כן, שימוש בציוד של מספר קטן של יצרנים עלול לפגוע בתחרות

19 בעת כתיבת מסמך זה עומדות בכך ארבע חברות: ZTE ו-Huawei הסיניות, Nokia ו-Ericsson. בשל החשש משימוש בציוד מתוצרת החברות הסיניות, בטווח הקצר יש להסתמך על Nokia ו-Ericsson.

ולא יעודד אותם לפעול לשיפור איכותם ויעילותם של מוצריהם. לפיכך, בטווח הארוך ראוי להגביר את תשומת הלב להתפתחויות בשוק ציוד התקשורת לרשתות 5G ולתת את הדעת על הופעתם של יצרנים חדשים, על אחת כמה וכמה לאור מאמצי הממשל האמריקני להכניס לשוק זה חברות אמריקניות (Stacy, 2019).

שמירה על חסינות שרשרת האספקה: כאמור, מורכבותן של שרשראות האספקה של רשתות 5G, הימצאם של ספקי הציוד וספקי המשנה, מתקני הייצור והקבלנים לעיתים קרובות במדינות שונות והכפפתם לרגולציות ולחוקים שונים, מקשים על המעקב אחר הציוד ועל ניטור חולשות האבטחה שבו. לפיכך מוצע לנסח מודל המדרג את רמת האמינות של היצרנים, הספקים וספקי המשנה על פי מאפיינים כגון תהליכי בקרת האיכות של היצרנים, שיטות עבודה מומלצות, תהליכי העבודה ומדיניות אבטחת הסייבר של היצרנים. במודל זה ייבחנו גם בדיקות רקע שעורך היצרן ותהליכי סינון העובדים שלו כדי לזהות תפיסות אידאולוגיות או פוליטיות, השתייכות או קרבה לארגוני פשע או לגופי ממשלה זרים שעלולים להוביל לחבלה בציוד או לריגול, חוקים לאומיים ורגולציות שהיצרן או ספקי המשנה כפופים אליהם במדינותיהם, היכולת של גופי ממשלה זרים להפעיל לחץ על היצרן או על ספקי המשנה ועוד.

שאלת האבטחה של שרשראות האספקה עלולה להוביל לדיון בנושא זהות הספקים. בישראל קיימת מדיניות בלתי רשמית של גורמי ההגנה בשירות הביטחון הכללי ובמשרד הביטחון לאסור מתן גישה לחברות סיניות לפרויקטים בענף התקשורת (זיו, 2018). אולם לשרשראות האספקה נשקפת סכנה גם מספקי המשנה. שרשראות האספקה של רשתות 5G יהיו תלויות בשבבים ובתוכנות – תחומים שבהם ליפן, לדרום קוריאה ולארצות הברית יתרונות של ממש על פני סין. עם זאת, לא מן הנמנע כי סין תשקיע מאמצים ומשאבים רבים (כגון כסף וריגול) כדי להדביק את הפער (5G supply chain security, 2020). נוסף על כך, השאלה מי מספק את הציוד לספקי המשנה תחייב לבצע בדיקות רקע וציוד גם לספקי המשנה לאורך שרשרת האספקה. בשל הקושי לפקח על ספקי משנה במדינות אחרות, ראוי להטיל רגולציה על ציוד קצה ומערכות תומכות ברשתות 5G (כגון מערכות תעשייתיות, מערכות ערים חכמות, תחבורה אוטונומית ובית חכם) בהיבטים של פיתוח מאובטח ותכנון והנדסה בראייה הגנתית, ולייצר תקן מדינה להיבט של הגנת סייבר למערכות תומכות ברשתות 5G.

יוזמה בין-לאומית חדשה שעשויה להוביל לשינויים מרחיקי לכת בשוק טכנולוגיות RAN היא יוזמת ה-RAN הפתוח (O-RAN). זוהי יוזמה של קבוצת חברות התקשורת המובילות בעולם, ומטרתה לפתח ארכיטקטורה וממשקים פתוחים עבור רשת RAN שתאפשר לחברות ולשחקנים חדשים להיכנס לשוק ולמפעילי הרשתות להסתמך על מספר רב יותר של ספקים. היוזמה צפויה עוד לאפשר ליותר טכנולוגיות RAN, שעד כה הסתמכו על חומרה ייעודית – תחום שבו יש לסין יתרון, להסתמך על תוכנות ועל וירטואליזציה – תחום שבו יש לארצות הברית יתרון. נוסף על כך, המעבר לשימוש בתוכנות גם בתחום RAN צפוי לספק גמישות, מִדְרגיות (scalability) ויכולת להוסיף משאבי מחשוב ולהקצות אותם בהתאם לדרישות כדי להתמודד עם עומס.

חברות ויצרניות של טכנולוגיות תקשורת כגון סיסקו וסמסונג, שבעבר נמנעו מלהיכנס לשוק טכנולוגיות RAN, הצטרפו ליוזמה זו ומעידות בכך על הפוטנציאל הטמון בה (Lewis, 2020, pp. 6–8; Rogers, 2019). עבור ישראל עשויה היוזמה לשמש הזדמנות בנושא ההתקנה והשימוש בתשתיות ובתקני RAN הנבחנים במסגרתה. שימוש בארכיטקטורה פתוחה יוכל לסייע לחברות

התקשורת הישראליות להסתמך על מספר רב של ספקים וכן להשתלב בשוק 5G ולהציע טכנולוגיות ופתרונות מקומיים.

החמרת תקני אבטחת הסייבר: מוצע לנסח תקני אבטחת סייבר לאומיים מחמירים שיחולו על האופן שבו יתופעלו וינוהלו הרשתות ויתמקדו בחסינות הרשתות, בהערכת סיכונים ובמתן מענה להם. על התקנים להבטיח את הנגישות והאמינות של הרשתות ושל השירותים המוצעים באמצעותן ואת סודיות המידע העובר ברשתות, ולהגן עליהן מפני גישה בלתי מאושרת או שיבוש. תקנים כאלה צריכים לשמש תנאי סף לאבטחת הרשתות, ועל מקבלי ההחלטות לעודד ולתמרץ את חברות התקשורת המפעילות את הרשתות להמשיך לבחון חידושים בתחום האבטחה כדי לספק אבטחה ברמה גבוהה יותר מהנדרש.

השתתפות בתהליכי תקנון בין-לאומיים: חולשות בפרוטוקולים, בארכיטקטורה של הרשתות ובפונקציונליות שלהן עלולות להיות תוצר של פוליטיזציה של תהליכי ניסוח התקנים הבין-לאומיים. ארגון 3GPP, המקיים את הליך התקנון הבין-לאומי המרכזי, מורכב מחברות ומומחים ממדינות שונות המציעים פתרונות טכניים שישמשו תקנים בין-לאומיים לטכנולוגיות תקשורת סלולרית. אולם העבודה המשותפת וההצבעה על פתרונות טכנולוגיים הפכו לזירה נוספת במאבק בין מדינות – ובראשן ארצות הברית וסין – ובתחרות הטכנולוגית ביניהן. כך נוצר מצב שבו חברות ומומחים מציעים פתרונות שנועדו להקנות לחברות המקומיות במדינות שאותן הם מייצגים יתרון תחרותי ואפשרות לרשום פטנטים על פתרונות שיישמו באופן נרחב בעולם, ועושים זאת לעיתים חֶלֶף קידום פתרונות יעילים אחרים.[20]

כיום חברות בארגון 3GPP 707 חברות מכ-44 מדינות; בארגון חברות תשע חברות ישראליות (החברות גם במכון התקנים האירופי לענף התקשורת, ETSI),[21] והן פועלות לצד 92 חברות אמריקניות ו-185 חברות סיניות (3GPP membership, n.d.). החדשנות והקִדמה של מדינת ישראל, בייחוד בתחום אבטחת הסייבר, יוכלו לתרום רבות לתהליך ניסוח התקנים, והגדלת מספר החברות הישראליות בארגון 3GPP תוכל להקנות לישראל רווח דיפלומטי והשפעה. כמו כן תוכל ישראל להרוויח מהשתתפות בפורומים בין-לאומיים העוסקים בעיצוב ארכיטקטורות חלופיות לטכנולוגיית 5G (כגון יוזמת O-RAN שהוזכרה לעיל).

מזעור סיכונים הנובעים מהגדלת שטח פני התקיפה: חולשות אבטחה אינן תלויות בהכרח בזהותם של הספק או היצרן, ולעיתים נובעות דווקא מתמריצי שוק, המציבים את העלויות מעל האבטחה בסדרי העדיפות של היצרנים. פתרונות רבים לכך מתבססים על ניסוח תקני אבטחת סייבר לייצור ולייבוא של מכשירי IoT, אולם דרישות אבטחה עלולות לייקר את שוק מכשירי IoT ולפגוע בתעשייה המקומית (פרוטוקול ישיבה מס' 160 של ועדת המדע והטכנולוגיה, 2018). נראה כי מעקב אחר המתרחש במדינות נוספות המגדירות את מצב אבטחת מכשירי IoT כאיום, ובמיוחד אחר המתרחש בארצות הברית בנושא, יוכל לסייע לישראל.

במאי 2020 פורסם מסמך ההמלצות של נציבות Cyberspace Solarium, נציבות שמינה הקונגרס האמריקני כדי לגבש המלצות לניסוח אסטרטגיית אבטחת סייבר לאומית. במסמך זה

20 דוגמה לכך מצויה בהצבעה שקיים הארגון ב-2016 לשם מציאת פתרון לקידוד מידע ופתרון לבעיות בשליחת נתונים. באותה הצבעה, לאחר שהופעל עליהם לחץ רב מצד ממשלת סין שינו נציגי חברת Lenovo הסינית את עמדתם ותמכו לבסוף בפתרון של חברת Huawei (Gorman, 2020).

21 European Telecommunication Standards Institute.

קוראת הנציבות לקונגרס לחוקק חוק שיחייב את יצרני מכשירי IoT להטמיע בהם אבטחת סייבר בסיסית ולהשתמש בתקנים למנגנוני אימות ולעדכון תוכנות (USA Cyberspace Solarium Commission, 2020, p. 2). אם חוק זה אכן יחוקק, סביר כי דרישתה של ארצות הברית מיצרני מכשירי IoT המעוניינים לספק את מוצריהם לממשלתה תוביל לשינויים בתהליכי הייצור של התעשייה ולהוזלתם של מכשירים מאובטחים, מהלך שגם ישראל והתעשייה המקומית יוכלו להרוויח ממנו.

סיכום

רשתות 5G נחוצות לישראל וחיוניות לביטחונה, לכלכלתה ולחברה הישראלית. יכולותיהן של הרשתות – העברת נתונים רבים וזמן המתנה קצר – צפויות לאפשר שינויים מהפכניים בתחומי הביטחון, הכלכלה, החינוך, הרפואה, קבלת ההחלטות והמשילות וכן בזירה הבין-לאומית. רשתות אלו צפויות לחזק ולעודד את החדשנות הישראלית, ולסייע בהפיכתה של מדינת ישראל מאומת סטארט-אפ (start-up nation) למשק טכנולוגי חכם (smartup nation) באופן שעשוי לשמר את מעמדה המוביל של ישראל בענפי הטכנולוגיות העתידיות בעולם.

עם זאת, בדומה לכל טכנולוגיית מידע ותקשורת, גם ברשתות 5G הובחנו חולשות ופערי אבטחה בתוכנות, בחומרה ובארכיטקטורה, והן חשופות לאיומי סייבר וריגול: ההסתמכות הראשונית של רשתות 5G על רשתות 4G עלולה לחשוף אותן לחולשות אבטחה ישנות; מורכבות שרשרת האספקה שלהן, ההסתמכות הגוברת על תוכנות ורכישת ציוד מספקים מועטים בלבד עלולים כולם לשמש גורמי איום. סביר כי שחקנים מדינתיים וגורמים א-מדינתיים, כגון ארגוני טרור ופשע, ינסו לנצל חסרונות אלה למטרותיהם. ככל שהכלכלה, הביטחון והחברה בישראל יסתייעו ביתרונות הטכנולוגיה וככל שתשתיות ושירותים חיוניים יסתמכו עליה, כך יגדל הנזק עקב שיבושים, תקלות וחבלה.

מאבק המעצמות בין ארצות הברית לסין – הבא לידי ביטוי גם בניסיון לאחוז במושכות ולהוביל את העולם בפיתוח ובמכירה של טכנולוגיות חדשות, בהן גם רשתות 5G – מעורר דיון בעולם ובישראל; זהו דיון חשוב וחיוני, אולם התמקדות יתר בשאלת זהות ספקי הציוד ובשאלות הפוליטיות העולות ממנה עלולה להסיט את תשומת הלב מהיבטים אחרים חשובים של פריסה והטמעה של רשתות 5G. כיום, למשל, הדיון בשימושים הפוטנציאליים של הטכנולוגיה מצומצם יחסית, ואינו מתמקד בצורך המתמיד לנטר ולבחון את הרשתות ולהיערך כראוי לקראת הנחת התשתיות, פריסתן, ניהולן והשימוש בהן.

במסמך זה פירטנו את היתרונות הגלומים בטכנולוגיית 5G ואת תרומתם לביטחונה הלאומי של ישראל, וקראנו לנסח גישה כוללת שתסייע להגן על הרשתות ולנהל את הסיכונים הנובעים מהן לאורך כל מחזור חייהן. על גישה כזו להתמקד באבטחת שרשראות האספקה של הרשתות, ולעקוב אחר יוזמות בין-לאומיות שיאפשרו כניסה של ספקים חדשים לשוק ואחר שינויי ארכיטקטורה שיאפשרו גמישות ומְדֻרגיות. על גישה כזו לתת את הדעת על חסינות הרשת, על ניסוח תקני אבטחה מחמירים עבור מפעיליה, על הצורך להרחיב את ההשתתפות בפורומים בין-לאומיים לניסוח תקנים ולאימוץ פטנטים עבור הרשת ולנסח מענה לאיומים פוטנציאליים על הרשתות.

מקורות

איזנברג, א' וזליבנסקי, ע' (2019). התאמת מערכת החינוך למאה ה-21 [תקציר מחקר]. המכון הישראלי לדמוקרטיה. https://www.idi.org.il/media/13079/adapting-israel-s-education-system-for-the-challenges-of-the-21st-centur.pdf

בן-ישראל, י' (2013). תפיסת הביטחון של ישראל. בן-שמן: מודן והאוניברסיטה המשודרת.

בן פורת, ע' (2019, 20 בפברואר). פס רחב מאוד: צה"ל נערך לדור 5. ערוץ 7. https://www.inn.co.il/News/News.aspx/394622

ברדה, ס' (2020, 10 במאי). מהפכת הדור החמישי של הסלולר. כלכליסט. https://www.calcalist.co.il/local/articles/0,7340,L-3819851,00.html

החדשנות הטכנולוגית כמנוע צמיחה מרכזי של ישראל. (ל.ת.). Luzzatto & Luzzatto Pattent Attornies. אוחזר ב-20 בספטמבר, 2020 מתוך https://www.luzzatto.co.il/מידע/מאמרים/החדשנות-הטכנולוגית-כמנוע-צמיחה-מרכזי-של-ישראל

החלטה 151 של הממשלה ה-34, "קידום הסוגיה האסטרטגית 'ישראל דיגיטלית' כנגזרת מהערכת המצב האסטרטגית כלכלית-חברתית לממשלה" (28.06.2015).

הלפרן, נ' (2020, 26 באוגוסט). OECD: התכווצות כלכלית חסרת תקדים ברבעון השני; מצב ישראל טוב יחסית. *The Marker*. https://www.themarker.com/wallstreet/.premium-1.9104021

התעשייה המסורתית מתחברת לחדשנות: רשות החדשנות ומשרד הכלכלה והתעשייה יתמכו בתעשייה המסורתית ב-125 מיליון ש"ח. (ל.ת.). *New-Tech*. אוחזר ב-20 בספטמבר, 2020 מתוך https://www.new-techonline.com/2018/01/התעשייה-המסורתית-מתחברת-לחדשנות-רשות

וייס, א' (2020). תמונת מצב המדינה: תרשימים בנושאי חברה וכלכלה בישראל. מרכז טאוב לחקר המדיניות החברתית בישראל. http://taubcenter.org.il/wp-content/files_mf/pon2020heb.pdf

ויסברג, ה' (2018, 29 בספטמבר). ישראל בין 6 המדינות היעילות בבריאות, אך יש גם חדשות רעות. גלובס. https://www.globes.co.il/news/article.aspx?did=1001254253

זיו, א' (2018, 26 בספטמבר). 'השב"כ לא יאשר': הסוד על חברות התקשורת מסין ורוסיה שרוצות לפעול בישראל. דה מרקר. https://www.themarker.com/technation/.premium-1.6509569.

חזן, א' (2014, 16 בנובמבר). לחנך כמו בפינלנד. *Ynet*. https://www.ynet.co.il/articles/0,7340,L-4592334,00.html

ינובסקי, א' (2020, 5 ביולי). אומת הסטארט-אפ פותחת פיגור בגלל היעדר תשתיות דור חמישי. *The Marker*. https://www.themarker.com/opinion/.premium-1.8959343

כהן, נ' (2018, 22 בדצמבר). הרחבת פרישת תשתית תקשורת סלולרית והיערכות לתחילת הפרישה של תשתית בדור החמישי [מכתב מנכ"ל משרד התקשורת אל מנכ"ל משרד הבריאות והמשרד להגנת הסביבה]. https://www.gov.il/BlobFolder/generalpage/09072019_01/en/Expanding%20the%20deployment%20of%20cellular%20communications%20infrastructure%20and%20preparing%20for%20the%20retirement%20of%20infrastructure%20in%20the%20fifth%20generation.pdf

לוי, א' (2016, 22 בנובמבר). חדשנות – לא מטרה, היא תהליך שלא נגמר, משתפר ומשתנה. גלובס. https://www.globes.co.il/news/article.aspx?did=1001162258

לוצאטו, א' (2019, 3 בספטמבר). ישראל מובילה במדד החדשנות הגלובאלי, אבל יש אבל. Geektime. https://www.geektime.co.il/wipo-proud/

מוסד שמואל נאמן (2017, מאי). אסטרטגיית-על למדינת ישראל: עיונים וכיוונים. חיפה: הטכניון.

מילרד, א' (2017, 18 ביוני). תשתיות אינטרנט: נתונים, תועלת כלכלית למשק וכל מדיניות לעידוד הקמתן. מרכז המחקר והמידע של הכנסת. https://fs.knesset.gov.il/globaldocs/MMM/b2b9b84c-3edb-e611-80cc-00155d0206a2/2_b2b9b84c-3edb-e611-80cc-00155d0206a2_11_10585.pdf

פרוטוקול ישיבה מס' 160 של ועדת המדע והטכנולוגיה, הכנסת ה-20 (19.2.2018). http://fs.knesset.gov.il/20/Committees/20_ptv_491710.doc

פרץ, ג' (2020, 5 בינואר). הדור החמישי: מכרז שתקוע כמו עצם בגרון לחברות הסלולריות, אבל אי אפשר בלעדיו. גלובס. https://www.globes.co.il/news/article.aspx?did=1001313624

קריסטל, מ' (2019, 31 בדצמבר). אהרון אהרון: "ישראל יכולה להיות מובילה בינלאומית ברפואה מותאמת אישית". כלכליסט. https://www.calcalist.co.il/conference/articles/0,7340,L-3776794,00.html

3GPP membership – Individual members (n.d.). Retrieved October 21, 2020 from https://webapp.etsi.org/3gppmembership/Results.asp?Member=ALL_PARTNERS&SortMember=Name&DirMember=ASC&SortPartner=Name&DirPartner=ASC&SortMarket=Name&DirMarket=ASC&SortObserver=Name&DirObserver=ASC&SortGuest=Name&DirGuest=ASC&Name=&search=Search

5G Barcelona (n.d.). 5G Connected Ambulance. https://5gbarcelona.org/pilots/5g-connected-ambulance

451 Research (n.d.). 5G impact on the financial services ecosystem. https://media2.mofo.com/documents/191003-spotlight-5g-payments.pdf

5G Americas (2018, October). *The evolution of security in 5G* [white paper]. https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_5G_Security_White_Paper_Final.pdf

Abraham Accords Peace Agreement: Treaty of Peace, Diplomatic Relations and Full Normalization Between the United Arab Emirates and the State of Israel, September 15, 2020, https://www.whitehouse.gov/briefings-statements/abraham-accords-peace-agreement-treaty-of-peace-diplomatic-relations-and-full-normalization-between-the-united-arab-emirates-and-the-state-of-israel/

Arias, R., Mauro, I., O'Halloran, D., Spelman, M., Deshmukh, M., Galal, H., Kabbara, M., Kaul, R., & Ratan, N. (2020, January). *The impact of 5G: Creating new value across industries and society* [white paper]. World Economic Forum & PWC. http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf

Asokan, A. (2020, March 30). Will 5G networks inherit vulnerabilities in 4G networks?. *Bankinfosecurity.* https://www.bankinfosecurity.com/will-5g-networks-inherit-vulnerabilities-in-4g-networks-a-14030

AT&T Business (n.d.). *5 Ways 5G Will Transform Healthcare.* Retrieved October 21, 2020, from https://www.business.att.com/learn/updates/how-5G-will-transform-the-healthcare-industry.html

Bieler, S. (2019, March 5). Market dynamics encourage weak security in consumer IoT. *Compliance & Enforcement.* https://wp.nyu.edu/compliance_enforcement/2019/03/05/market-dynamics-encourage-weak-security-in-consumer-iot/

Bureau of Communications, Arts and Regional Research (2018, April 9). *Impacts of 5G on productivity and economic growth* [working paper]. Australian Government Department of Infrastructure, Transport, Regional Development and Communications. https://www.communications.gov.au/departmental-news/impacts-5g-productivity-and-economic-growth

Burnham, C. (2019, April 12). 5G Is the essential security imperative of our time. *Forbes.* https://www.forbes.com/sites/christopherburnham/2019/04/12/5G-is-the-essential-national-security-imperative-of-our-time/#48d670712c22

Chong, A. (2010). Small state soft power strategies: Virtual enlargement in the cases of the Vatican City state and Singapore. *Cambridge Review of International Affairs, 23(3), 383–405.*

Condoluci, M., & Mahmoodi, T. (2018, December). Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges. *Computer Networks, 146, 14–16.* https://nms.kcl.ac.uk/toktam.mahmoodi/files/sdn-nfv-5G-survey.pdf

Deloitte (2019, August). *Scotland's digital potential with enhances 4G and 5G capability: Final report for Scottish futures trust.* https://www.scottishfuturestrust.org.uk/storage/uploads/deloittesfteconomicimpact4g5gfinalreportforpublication.pdf

Dettling, L. J. (2017). Broadband in the labor market: The impact of residential high-speed internet on married women's labor force participation. I*LR Review, 70(2), 452–482.*

Dignan, L. (2019, June 18). *IoT devices to generate 79.4zb of data in 2025, says* IDC. ZDNet. https://www.zdnet.com/article/iot-devices-to-generate-79-4zb-of-data-in-2025-says-idc/

Duffy, S. (n.d.). *5G: A transformative technology.* Barclays. https://www.barclayscorporate.com/content/dam/barclayscorporate-com/documents/insights/innovation/5g-a-transformative-technology.pdf

Dutta, S., Lanvin, B., & Wunsch-Vincent, S. (2019). *Global innovation index 2019 report: Creating healthy lives – The future of medical innovation.* WIPO. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2019.pdf

Ekström, H. (2019, July 11). Non-standalone and standalone: Two standards-based paths to 5G. *Ericsson Blog.*

Ericsson (2018, January). *The industry impact of 5G: Insights from 10 sectors into the role of 5g.* https://files.vogel.de/vogelonline/vogelonline/files/9763.pdf

Eurasia Group. (2018, November 3). *The geopolitics of 5G [*white paper]. https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf

Federal Ministry of Transport and Digital Infrastructure (2017, July). *5G strategy for Germany.* The German Federal Government. https://www.bmvi.de/SharedDocs/EN/publications/5g-strategy-for-germany.pdf?__blob=publicationFile

Gat, A. (2006). *War in human civilization.* Oxford, UK: Oxford University Press.

Gorman, L. (2020, April 2). The U.S. needs to get in the standards game – with like-minded democracies. *Lawfare.* https://www.lawfareblog.com/us-needs-get-standards-game%E2%80%94-minded-democracies

Gruber, H., Hätönen., J., & Koutroumpis, P. (2014). Broadband access in the EU: An assessment of future economic benefits. *Telecommunications Policy, 38(11), 1046–1058.*

GSMA (2018, December). *Study on socio-economic benefits of 5G services provided in mmWave bands.* https://www.gsma.com/spectrum/wp-content/uploads/2019/10/mmWave-5G-benefits.pdf

KPMG. (2020, June). The 5G edge computing value opportunity. https://assets.kpmg/content/dam/kpmg/co/sac/pdf/2020/07/5g-edge-computing-value-opportunity.pdf

Kennedy, D. (2019, July 26). The facts on 5G: How 5G networks are being built in the real world. *Ovum.* https://www.ericsson.com/49472a/assets/local/reports-papers/white-papers/the-facts-on-5G-final-report.pdf

Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security threats and best practices. *IEEE Communications Magazine, 55(8), 2–8.*

5G supply chain security: Threats and solutions, U. S. Senate Committee on Commerce, Science and Transportation, Cong. (2020a) (testimony of James A. Lewis). https://www.commerce.senate.gov/services/files/563D903B-FEF0-4A1C-9202-A7DC1CCEFC6F

Lewis, J. (2020, June). *Can telephones race? 5G and the evolution of telecom* (part 1). Center for Strategies and International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/20615_Lewis_TelephoneRace_WhitePage_v2_FINAL.pdf

Lichtman, M., Rao, R., Marojevic, V., Reed, J., & Jover, R. P. (2018, May 20–24). 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation [1st workshop]. I*EEE International Conference on Communications Workshops (ICC* Workshops), Kansas City, MO, USA. https://arxiv.org/pdf/1803.03845.pdf

Little, A. D. (2017). *Creating a gigabit society – The role of 5G.* Vodafone Group. https://www.vodafone.com/content/dam/vodcom/files/public-policy/gigabit-society-5g-04042017.pdf

Lourenço, M., & Marinos, L. (Eds.) (2019, November 21). *Threat landscape for 5g networks* [ENISA Report]. European Union Agency for Cybersecurity [Enisa] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/at_download/fullReport

Marinho, J. (2019, June 12). What's new in 5G security? A brief explainer. *CTIA* https://www.ctia.org/news/whats-new-in-5G-security-a-brief-explainer

Martin, A., Marinos, L., Rekleitis, E., Spanoudakis, G., & Petroulakis, N. (2015, December). *Threat landscape and good practice guide for software defined networks/5G* [ENISA Report]. European Union Agency for Cybersecurity [Enisa] https://openaccess.city.ac.uk/id/eprint/15504/7/SDN%20Threat%20Landscape.pdf

Mirzamany, E., Neal, A., Dohler, M., & Rosas, M. L. (n.d.). *5G and education.* Jisc. https://community.jisc.ac.uk/sites/default/files/Education-VM_Extended.pdf.

Nakarmi, P. K. (2019, January 18). 3GPP release 15: An end to the battle against false base stations? *Ericsson Blog.* https://www.ericsson.com/en/blog/2019/1/3gpp-release15

Gunnerson, B., & Reall, B. (n.d.). *What is a small cell and why does it matter.* Gunnerson Consulting & Communication Site Services. Retrieved October 21, 2020, from https://www.gunnersonconsulting.com/what-is-a-small-cell-why-does-it-matter

Haddix, J. (2019, January 8). Your life is the attack surface: The risks of IoT. *DarkReading.* https://www.darkreading.com/endpoint/your-life-is-the-attack-surface-the-risks-of-iot-/a/d-id/1333588

Hamilton, I. A. (2020, February 12). The US says Huawei has been spying through 'back doors' designed for law enforcement – which is what the US has been pressuring tech companies to do for years. *Business Insider.* https://www.businessinsider.com/us-accuses-huawei-of-spying-through-law-enforcement-backdoors-2020-2

Highroad Team (2020, August 16). 5G – The network of Israel's future or Israel's future undoing? *Highroad.* https://blog.highroad.center/5g-the-network-of-israels-future-or-israels-future-undoing/

Hoehn, J. R., & Sayler, K. M. (2020, June 4). *National security implications of fifth generation (5G) mobile technologies.* Congressional Research Service https://fas.org/sgp/crs/natsec/IF11251.pdf

Hogg, S. (2014, October 28). SDN security attack vectors and SDN Hardening. *Networkworld.* https://www.networkworld.com/article/2840273/sdn-security-attack-vectors-and-sdn-hardening.html

Hussain, S. R., Echeverria, M., Chowdhury, O., Li, N., & Bertino, E. (2019, February *24–27). Privacy attacks to the 4G and 5G cellular paging protocols using side channel information* [Paper presentation]. 26th Annual Network and Distributed System Security Symposium, San Diego, CA, United States. https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_05B-5_Hussain_paper.pdf

Jamshidi, S. (n.d.). *Extended reality and O2O communications.* The Optical Zeitgeist Laboratory. Retrieved October 21, 2020, from http://www.zeitgeistlab.ca/doc/Extended_Reality_and_O2O_Communications.html

Yen, H., Simpson, D., & Gorman, L. (2020, Spring). *Tech factsheets for policymakers: 5G* (A. Jayanti, Ed.). Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/files/publication/5G_2.pdf

Jones, J. L. (2019, February 11). *Strategic insights: Recommendations on 5G and national security* [Memo no. 3]. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2019/09/Strategic_Insights_Memo_vF_2.11.pdf

Karabeshkin, L., & Rusetski, R. (2013). Estonia's soft power. *Baltic Horizons, 20(117), 45–52.*

Newman, L. H. (2019, August 3). 5G is here – and still vulnerable to stingray surveillance. *Wired*. https://www.wired.com/story/5G-security-stingray-surveillance/

NIS Cooperation Group. (2019, October 9). *EU coordinated risk assessment of the cybersecurity of 5g networks [*report]. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

Nokia. (2016). *5G use cases and requirements* [white paper]. https://www.ramonmillan.com/documentos/bibliografia/5GUseCases_Nokia.pdf

Nye, J. S. (2004). *Soft power: The means to success in world politics.* New York: Public Affairs.

Nye, J. S. (2019). Soft power 2.0: The future of power in the digital age. *Dubai Policy Review, 1, 11–14.* https://dubaipolicyreview.ae/soft-power-2-0/

Organisation for Economic Co-operation and Development [OECD]. (2019). *Pisa 2018 results: Combined executive summaries* (Vol. I–III). https://www.oecd.org/pisa/Combined_Executive_Summaries_PISA_2018.pdf

Organisation for Economic Co-operation and Development [OECD] & Statistical Office of the European Communities [Eurostat]. (2005). *Oslo manual: Guidelines for collecting and interpreting innovation data* (3rd ed.). Paris: OECD Publishing.

Osher, L., & Ivri, N. (2019, August 26). *5G in Israel: Window of opportunity for western multinational telecoms?* APCO Worldwide. https://apcoworldwide.com/blog/5g-in-israel-window-of-opportunity-for-western-multinational-telecoms/

Oxford Economics. (2019, December). *Restricting competition in 5g network equipment: An economic impact study*. https://resources.oxfordeconomics.com/hubfs/Huawei_5G_2019_report_V10.pdf

Positive Technologies. (2020, June). *Threat vector: GTP – Vulnerabilities in LTE and 5G Networks 2020*. https://positive-tech.com/storage/articles/gtp-2020/gtp-2020-eng.pdf

Press Trust of India [PTI]. (2020, September 8). India, US, Israel collaborating in 5G tech: official. *The Times of India.* https://timesofindia.indiatimes.com/business/international-business/india-us-israel-collaborating-in-5g-tech-official/articleshow/77989007.cms

Prieger, J. E. (2020, February). *An economic analysis of 5G wireless deployment: Impact on the U.S. and local economies.* The App Association [ACT]. https://actonline.org/wp-content/uploads/ACT-Report-An-Economic-Analysis-of-5G-FINAL.pdf

Rogers, M. (2019, January 7). The new wave of telecoms: How open RAN may cause major vendor shakeup. *IT Connection.* https://itcblogs.currentanalysis.com/2019/01/07/the-new-wave-of-telecoms-how-open-ran-may-cause-major-vendor-shakeups/

Röpke, C., & Holz, T. (2015, November). SDN rootkits: Subverting network operating systems of software-defined networks. *RAID.* https://www.ei.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2016/01/14/SDN-Rootkit_RAID15.pdf

Schneier, B. (2020, January 10). China isn't the only problem with 5G. *Foreign Policy.* https://foreignpolicy.com/2020/01/10/5G-china-backdoor-security-problems-united-states-surveillance/

Schwab, K. (2019). *The global competitiveness report 2019.* World Economic Forum. http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

Shaghaghi, A., Kaafar, M. A., Buyya, R., & Jha, S. (2020). Software-defined network (SDN) data plane security: Issues, solutions, and future directions. In B. Gupta, G. M. Perez, D. P. Agrawal, & D. Gupta (Eds.), *Handbook of computer networks and cyber security (341–387)*. Switzerland: Springer.

Stacy, K. (2019, October 8). US pushes to fund western rivals to Huawei. *Financial Times*. https://www.ft.com/content/94795848-e6e3-11e9-b112-9624ec9edc59

Sullivan, J., & Lucas, R. (2020, February). *5G cyber security: A risk-management approach.* Royal United Services Institute for Defence and Security Studies. https://rusi.org/sites/default/files/20200602_5G_cyber_security_final_web_copy.pdf

Teppo, P., & Norrman, K. (2020, April). *Security in 5G RAN and core deployments* [Ericcson white paper]. Ericcson. https://www.ericsson.com/49a5ea/assets/local/reports-papers/white-papers/ericsson-whitepaper-5Gran.pdf

Transparency International (2020, January). *Corruption perceptions index 2019.* https://www.transparency.org/files/content/pages/2019_CPI_Report_EN.pdf

UK Department for Digital, Culture, Media & Sport. (2018, March 7). *Secure by design: Improving the cyber security of consumer Internet of Things report* [policy paper].https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf

USA Cyberspace Solarium Commission. (2020, May 2). *Cybersecurity lessons from the pandemic* [CSC white paper no. 1]. https://drive.google.com/file/d/1wCHVtIFlw84uZIPOTZe2nkdGau15fLAQ/view

Verizon (2019, November 18). *What is the difference between 3G, 4G and 5G?* https://www.verizon.com/about/our-company/5g/difference-between-3g-4g-5g

Wang, T. (2016). Benefits and the security risk of software defined networking. *ISACA Journal, 4,* 25–27. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/benefits-and-the-security-risk-of-software-defined-networking

Whitacre, B., Gallardo., R., & Strover, S. (2014). Broadband's contribution to economic growth in rural areas: Moving towards a causal relationship. *Telecommunications Policy, 38(*11), 1011–1102.

Wheeler, T., & Simpson, D. (2019, September). *Why 5G requires new approaches to cybersecurity.* Brookings. https://www.brookings.edu/research/why-5G-requires-new-approaches-to-cybersecurity/

Whittle, N. (2019, November 18). How 5G could transform the delivery of healthcare. *Cambridge Wireless.* https://www.cambridgewireless.co.uk/news/2019/nov/18/how-5g-could-transform-delivery-healthcare/

Williams, R. (2019, July 15). *Securing 5G networks: Challenges and recommendations*. Council on Foreign Relations. https://www.cfr.org/report/securing-5G-networks

Zaballos, A. G., Rodriguez, E. I., Kim, K. W., & Park, S. (2020). *5G: The driver for the next-generation digital society in Latin America and the Caribbean*. Inter-American Development Bank [IDB]. https://publications.iadb.org/publications/english/document/5G_The_Driver_for_the_Next-Generation_Digital_Society_in_Latin_America_and_the_Caribbean.pdf

טכנולוגיית הדור החמישי (5G) של הרשתות הסלולריות עומדת במרכזו של דיון תקשורתי נרחב בעולם ובישראל עקב השינויים והמהפכות שהיא צפויה לקדם בתחומי חיים רבים. מלבד תחום התקשורת, רשתות 5G צפויות לתמוך בפתרונות טכנולוגיים גם בתחומי הביטחון, הרפואה, החינוך והחברה, וכן לתרום לצמיחה כלכלית ולהשפיע על תהליכי קבלת החלטות.

על אף יתרונותיה הרבים, גם ברשתות 5G הובחנו חולשות ופערי אבטחה בתוכנות, בחומרה ובארכיטקטורה והן חשופות לאיומי סייבר וריגול. כמו כן, גם מאפיינים המבדילים את רשתות 5G מרשתות מדורות קודמים, כגון מורכבות שרשראות האספקה שלהן, ההסתמכות הגוברת על תוכנות ורכישת ציוד מספקים מועטים בלבד עלולים לשמש גורמי איום. אלו צפויים להיות מנוצלים על ידי שחקנים מדינתיים כגון ממשלות וגופי מודיעין זרים וכן על ידי גורמים א-מדינתיים, כגון ארגוני פשע וטרור.

הדיון הנרחב שעוררו רשתות 5G על רקע התחרות בין ארצות הברית וסין, הבא לידי ביטוי בדרישתה של ארצות הברית מבעלות בריתה – וביניהן ישראל – להימנע מרכישה ומשימוש בציוד תקשורת מתוצרת סין, הסיט את תשומת הלב מהיבטים חשובים אחרים, כגון הדיון בשימושים הפוטנציאליים של הטכנולוגיה, באיומים עליה ובדרך למזערם. לפיכך, מציג מאמר זה את היתרונות הגלומים בטכנולוגיה ואת תרומתה לישראל וכן את איומי הסייבר והריגול השונים הנלווים לה. לבסוף, מציע מאמר זה דרכי פעולה אפשריות להתמודדות עם האיומים.

עמרי וקסלר הוא חוקר בכיר למדיניות ולאסטרטגיית סייבר ואחראי פרויקט הסייבר של סדנת יובל נאמן למדע, טכנולוגיה וביטחון.

דורון פלדמן הוא דוקטורנט בבית הספר למדע המדינה, ממשל ויחסים בין-לאומיים באוניברסיטת תל אביב.

סדנת יובל נאמן למדע, טכנולוגיה וביטחון

הוקמה בשנת 2002 על ידי פרופסור אלוף (במיל.) יצחק בן ישראל, בשיתוף 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.

ICRC
Blavatnik Interdisciplinary Cyber Research Center

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

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