

עד כמה ללחוץ על דוושת הגז – המרוץ לפיתוח מכונית אוטונומית בשוה

אנדרו טאבאס

להופעת המכונית האוטונומית יש השלכות מרחיקות לכת בתחומים שונים, כמו הבעלות על הרכב, מערך התחבורה והבטיחות. כבר כיום יכולים האקרים להשתלט על מכונית אוטונומית דרך מערכות הניווט או הבידור שלה. חיבור מכוניות אוטונומיות לרשת יאפשר להשתלט עליהן במספרים גדולים. לפיכך, מקבלי ההחלטות חייבים לפעול כבר עתה כדי ליישם מנגנוני אבטחה טכניים ומשפטיים שימנעו מצב כזה. פתרונות אפשריים הם הקמה של מערכת אישורים, מאמץ ליצור "מרווח אוויר" בין רשתות המחשב השונות ברכב האוטונומי וחקיקת חוקי עונשין להאקרים. למרות הסיכונים הכרוכים במכונית האוטונומית, אל ליצרנים להירתע מפיתוח. במקום זאת, עליהם להיות המובילים במרוץ לפיתוח טכנולוגיה שתתגבר על סיכונים אלה.

מילות מפתח: מכונית אוטונומית, מכונית ללא נהג, V2V, V2I, מערכות תחבורה חכמות, האינטרנט של הדברים, הצפנת מפתח ציבורי, אבטחת סייבר, האקר, מרווח אוויר

מבוא

בסיפור הקצר "סאלי" שכתב אייזק אסימוב ב־1953, הוא מתאר מכוניות "פוזיטרוניות" שנוסעות בעצמן. המכוניות גם מתקשרות ביניהן (ברשת של כלי רכב אוטונומיים), מגינות על עצמן (בתגובה לחששות אבטחה) והורגות (דבר הממחיש את הבעיות האתיות המתעוררות סביב רכבים אוטונומיים)¹. "סאלי" הוא נקודת פתיחה טובה לדיון במכוניות אוטונומיות (AV), מכיוון שהסיפור מצביע על סוגיות שחברות טכנולוגיות ויצרני רכב מתמודדים אתן כבר היום.

אנדרו טאבאס הוא בעל תואר ראשון ביחסי חוץ מטעם אוניברסיטת ג'ורג'טאון, ואנליסט בקבוצת קדמוס.

רכב אוטונומי הוא בעל פגיעויות ייחודיות שמצריכות פתרונות אבטחה חדשניים. ראשית, מכונית אוטונומית תלויה בחיישנים לקבלת הקלט. חיישנים אלה יכולים לקבל קלט מוטעה וכך לסכן את ביטחון הרכב ונוסעיו; שנית, מכונית אוטונומית מקבלת מידע הנוגע למצבים של חיים ומוות – מערכות GPS, עדכוני חומרה קריטיים ותקשורת עם כלי רכב אחרים. מידע זה נובע ממערכת שנשענת על תשתית ענן, ויכולה לפיכך להיות חשופה להשתלטות של האקרים. יצרני מכוניות אוטונומיות אינם צריכים להירתע מאתגרים אלה, שכן המנצח במרוץ לפיתוח מכונית אוטונומית בטוחה ומוגנת יצליח להציל חיים ולשנות את העולם.

השכנוולוגיה

כדאי להבחין בין "מכונית אוטונומית" ובין "מכונית ללא נהג" (self-driving car). מכוניות אוטונומיות יכולות לנהוג לבד בתנאים מסוימים, אולם שומרות על יכולת הנהיגה האנושית. מכוניות אוטונומיות חייבות להציע "נסיגה חלקה" ממצב אוטונומי, דהיינו מעבר חלק לנהג האנושי.² פיתוח של מכוניות אוטונומיות מיטיב עם יצרני הרכב, משום שהוא מאפשר להם להתפאר ולפרסם כי כלי הרכב שהם מייצרים הינם בעלי טכנולוגיות מתחכמות.

לעומת המכונית האוטונומית, מכוניות ללא נהג לא יאפשרו לבני אדם לנהוג בהן. הן גם ייראו שונות במובהק מהמכוניות של ימינו, בכך שיהיו נטולות הגה, דוושות ומראות. מכוניות ללא נהג אף יוכלו ליצור "צי של רכבים שיתופיים" שישים קץ לבעלות המסורתית על כלי רכב.³ מכוניות ללא נהג יהוו איום על יצרני הרכב המסורתיים, ויביאו לכך שמכוניות משפחתיות יהפכו לפריט יוקרה. חברת "טסלה", המפתחת מכונית אוטונומית, כבר הציעה שבעלים של מכונית אוטונומית יוכלו להרוויח כסף באמצעות שילובה בצי של כלי רכב אוטונומיים כאשר היא לא תהיה בשימוש של בעליה. לדברי החברה, רעיון זה יסייע להוזיל את מחיר המכונית האוטונומית.⁴

מינהל בטיחות הדרכים האמריקאי (NHTSA) מציין חמש רמות של אוטומציה: "ללא אוטומציה" (0); "אוטומציה בפונקציה ייחודית" (1); "אוטומציה בפונקציות משולבות" (2); "אוטומציית נהיגה מוגבלת" (3); "אוטומציית נהיגה מלאה" (4). רמה גבוהה יותר פירושה יותר פונקציות של המכונית שאינן דורשות התערבות של נהג אנושי. רמה 0 מייצגת את המכונית המסורתית; ברמה 1 המכונית יכולה לבצע בעצמה כמה משימות ספציפיות; ברמה 2 היכולות האוטונומיות של הרכב מסוגלות להשתלב זו בזו, אולם הנהג עדיין חייב להיות פעיל. לדוגמה, מכונית ברמה 2 יכולה לשלב "בקרת שיוט מותאמת" עם "מרכז נתיב"; כלי רכב ברמה 3 יכולים לנהוג בעצמם בסביבות מסוימות, אולם הנהג חייב להישאר ערני⁵ (אם כי ייתכן שנהגים יתקשו להישאר מרוכזים כאשר המכונית האוטונומית עושה את מרבית

העבודה); ברמה 4 הנהג אינו צריך להישאר ערני ואף אינו צריך להישאר ברכב.⁶ מכוניות ברמה 4, שהן למעשה מכוניות ללא נהג, אינן זקוקות כאמור להתקנת הגה, דוושות או שאר המרכיבים המוכרים לנו במכוניות כיום.

במכונית המסורתית, נהגים אנושיים הם הקישור בין הרכב לסביבתו: הם משגיחים על תמרורים ורמזורים, שמים לב לתנאי הדרך, נמנעים מלהתקרב לכלי רכב אחרים, מתקשרים עם נהגים אחרים ומנווטים את דרכם. כדי למלא פונקציות אלו, המכונית האוטונומית עושה שימוש בחיישנים, בתקשורת "רכב לרכב" (V2V) ובתקשורת "רכב לתשתית" (V2I). כמו האינטרנט של הדברים (IoT), גם המכונית האוטונומית מסתמכת על תשתית ענן.

"מערכות החישה" שמספקות את המידע למכונית האוטונומית, המתוארות על ידי אנדרסון ושותפיו, כוללות את המצלמות שאוספות נתונים על העולם שבחוץ⁷ אך מוגבלות בשל תנאי מזג אוויר ויכולת התוכנה להמיר תמונות לנתונים,⁸ וכן חיישנים – חיישני מכ"ם ולידאר, המפיקים אות ועוקבים אחר הזמן שלוקח לו לפגוע באובייקט ולחזור לחיישן כדי לקבוע את המרחק ממנו.⁹ לשתי טכנולוגיות החיישנים יש מגבלות, משום שחלק מהמשטחים אינם מחזירים כהלכה גלי רדיו ואור.¹⁰ חיישנים על-קוליים מזהים אובייקטים קרובים, ואילו חיישני אינפרא-אדום מזהים אובייקטים בלילה.¹¹ מכוניות אוטונומיות יכולות להשתמש גם במערכות GPS ובמערכות ניווט פנימיות (INS) לצורך השגת מידע על מיקומן.¹² מערכת INS נשענת על ג'ירוסקופים, מדי גובה ומדי תאוצה.¹³ בנוסף, למכונית אוטונומית יש גישה למפות שכוללות מידע על רמזורים.¹⁴ לדוגמה, חברת "גוגל" תכננה כלי רכב שאוספים מידע ובונים מפות וירטואליות של מאפייני הדרך תוך כדי הנסיעה.¹⁵

מכוניות אוטונומיות מתקשרות עם רשתות כלי רכב זמניות (VANET).¹⁶ רשתות VANET "הן הבסיס למערכות תחבורה חכמות (ITS)".¹⁷ טכנולוגיות של "רכב לתשתית" (V2I) משתפות בין המכוניות מידע על רמזורים ושאור גורמים חיצוניים ומסייעות לרכב האוטונומי להבין את העולם מסביבו. ניתן להשתמש בבלוטות' כדי לשפר תקשורת V2I.¹⁸ טכנולוגיות "רכב לרכב" (V2V) מאפשרות למכוניות לשתף ביניהן מידע בנוגע למיקום ולמהירות של כל אחת מהן, ובכך לצמצם את הסיכוי לתאונה. מכוניות אוטונומיות מתקשרות האחת עם השנייה באמצעות תקשורת ייעודית לטווח קצר (DSRC).¹⁹ לאחרונה פרסם מבקר המדינה של ארצות הברית מחקר על היישום האפשרי של טכנולוגיות במכוניות עם נהגים אנושיים.²⁰

מכונית אוטונומית מתבססת על "חישה-תכנון-פעולה".²¹ המכונית מזהה מידע, מריצה אלגוריתמים כדי לקבוע את התגובה המיטבית ומוציאה לפועל את הפעולה הדרושה. מכונית אוטונומית היא דוגמה ל"מערכות עם שילוב מסיבי של מתמרים

חכמים" (MIST), אשר "עושות שימוש ברעיונות הענן כדי לקלוט מידע, לחוש את הסביבה ולהשתלב בצורה פעילה במצב במטרה להשיג את התוצאה הרצויה".²² מכוניות אוטונומיות מציבות אתגר ייחודי, משום שעליהן להבטיח את בטיחות הנוסעים בכל מחיר. לפיכך, על מהנדסי המכוניות האוטונומיות להבטיח כי החיישנים שבהן יהיו אפקטיביים בכל מצבי מזג אוויר ותנאי דרך. כמו כן, עליהם להגן על חיישנים אלה מפני התערבות חיצונית שעלולה לאיים הן על בטיחות הנוסעים ברכב האוטונומי והן על אלה שבכלי הרכב שסביבו. מסיבה זו, אבטחת הסייבר הופכת לגורם מרכזי בייצור מכוניות אוטונומיות.

לקראת רשת קולקטיבית של כלי רכב

תקשורת מסוג "רכב לרכב" (V2V) או "רכב לתשתית" (V2I) מאפשרת ליצור רשת קולקטיבית של כלי רכב. כדי ליצור מכונית יעילה, על בני האדם, המכוניות והתשתיות לדבר אלה עם אלה. המכוניות ילמדו על תנאי מזג האוויר ומידע נוסף דרך תשתית הענן. בשלב הראשון הן יאלצו להתמודד עם נהגים אנושיים, אולם בסופו של דבר הן יתקשרו אך ורק האחת עם השנייה. ברשת נטולת נהגים אנושיים יידרשו המתכנתים לקבוע שיטות להגדלת זרם התנועה. לפי Riener, עתיד המכונית האוטונומית הוא בצי שיתופי שבו הנוסע יוכל להזמין רכב לנסיעה, ולאחר מכן לשחרר אותו ולאפשר לו לחזור למיקום מרכזי ייעודי.²³

בדומה לחיישנים, גם תקשורת "רכב לרכב" או "רכב לתשתית" מציבה אתגרים של אבטחת סייבר. תקשורת זדונית עלולה להסתיר סיכונים דרך או להמציא כאלה. סיכונים מומצאים מסוג זה יגרמו למכונית להתנהג באופן בלתי צפוי. האקרים משוכללים יותר עלולים לנצל את מערכת התקשורת של המכונית האוטונומית כדי לקבל דרכה גישה למחשב המרכזי שלה, וכך להשיג שליטה על ההיגוי והבלמים של הרכב. לכן, חיוני לאבטח את כל מסרי התקשורת ששולחת המכונית האוטונומית.

מגמות עכשוויות בתעשייה

המרוץ לפיתוח מכונית אוטונומית בטוחה משותף הן ליצרני הרכב המסורתיים והן לחברות טכנולוגיה, ובהן "פולקסווגן", "מרצדס בנץ", "טסלה", "בוש", "אובר", "לוקהיד מרטין", "גוגל", "אפל" ואחרות. הפיתוח של מכוניות אוטונומיות התרחב, וכיום הוא כולל משאיות וכלי רכב צבאיים.²⁴ אלון מאסק, מייסד "טסלה", העריך לא מכבר שעד שנת 2030 או 2035 מרבית המכוניות יהיו אוטונומיות.²⁵ חברת "אובר" הקימה לאחרונה מעבדה בפיטסבורג, שם שוקד מספר רב של בוגרי אוניברסיטת "קרנגי מלון" על חקר מכוניות ללא נהג. חברת "גוגל" שיגרה בינתיים לכבישים מכוניות ללא נהג שכבר גמאו 300,000 מיילים מבלי לגרום לאף תאונה.²⁶

לכל אחד מיצרני הרכב המסורתיים ולחברות הטכנולוגיה יש יתרונות שונים, הגורמים לוויכוחים מי מהם יצליח יותר. חברות הרכב המסורתיות מותאמות טוב יותר לטפל באתגרים הייחודיים הנוגעים לייצור מכוניות, ויכולות לשלב בהן בהדרגה מאפיינים חדשים. לעומתן, חברות הטכנולוגיה המבקשות להשתלב בשוק הרכב עשויות להיתקל בקשיים מצד המשתמשים. למרות זאת, אחד ממנהלי "גוגל" טוען שתוכנית החברה לעבור למכירה של מכוניות אוטונומיות מלאות עשויה להתגלות כאסטרטגיה עסקית יעילה.²⁷

יצרני המכוניות האוטונומיות יהיו חייבים להשיג את הסכמת המשתמשים, וזאת באמצעות עיצוב חדשני, בטיחות מתקדמת ונתונים סטטיסטיים שיובאו לידיעת הציבור: ראשית, צריך שהתצוגה שתחליף את ההגה במכוניות ללא נהג (מכוניות ברמה 4 לפי סולם NHTSA) תשרה תחושת ביטחון ברכב;²⁸ שנית, מומחי אבטחה יהיו חייבים לקחת בחשבון את הסיכונים של פריצה לנתונים ושל מתקפה ישירה על מערכות הרכב. בשימוע בקונגרס האמריקאי שהוקדש לנושא זה הכירו הדוברים בכך ש"השתלטות האקרים עלולה לאיים על היכולת להגיע לשיעור הסכמה גבוה" כלפי מכוניות אוטונומיות, וזאת ככל שיתגבר החשש מפני אבטחת נתונים ובטיחות אישית.²⁹ במצב כזה, המשתמשים יהיו מודאגים מהאפשרות שהתקשורת "רכב לרכב" בכלי הרכב שלהם לא מוגנת,³⁰ וגם יחששו מפני מתקפות שיפגעו בבטיחות הפעולה של המכונית עצמה; שלישית, יצרנים יוכלו להדגיש את העובדה שמכוניות חכמות בטוחות יותר ממכוניות שנהוגות בידי אדם.³¹ 93 אחוזים של תאונות הדרכים בארצות הברית בשנת 2012 נגרמו בשל טעות אנוש, גבו את חייהם של 34,080 בני אדם³² ועלו כמעט 230 מיליארד דולר למשק האמריקאי.³³ מכוניות אוטונומיות יוכלו לסייע במעבר ל"מטרת העל", שהיא "מערכת התחבורה היעילה והבטוחה ביותר שניתן להעלות על הדעת".³⁴ עם זאת, במקרה שמכונית אוטונומית בכל זאת תעשה תאונה, סביר להניח שאמצעי התקשורת ידונו באירוע זה יותר מאשר במקרה של תאונה עם מכונית רגילה. לדוגמה, המוות הראשון אי פעם בתאונה שעירבה מכונית אוטונומית התרחש ביוני 2016, כאשר מכונית "טסלה" התנגשה בנגרר של טרקטור בעת פנייה.³⁵ התאונה קיבלה כיסוי תקשורתי ניכר, אך חברת "טסלה" הזדרזה להרגיע את הציבור כי אפילו לאחר התאונה, שיעור מקרי המוות של מנגנון הנהג האוטומטי נמוך יותר מזה של הנהג האנושי.³⁶

דרך נוספת להעלות את שיעור "הסכמת המשתמש" היא באמצעות הדגשת היתרונות הנוספים של המכונית האוטונומית. באלה ניתן לכלול ניידות רבה יותר של אנשים שאינם מסוגלים לנהוג, הקטנת התלות בחניה וכן יתרונות סביבתיים פוטנציאליים.³⁷ היצרנים צריכים להדגיש שיתרונות אלה עולים במשקלם על

העלייה הפוטנציאלית בסך הקילומטרים שניסע ועל הירידה הצפויה במספר מקומות העבודה עבור נהגים מקצועיים.³⁸

פגיעויות

השתלטות של האקרים על מכוניות כיום הינה גם לא יעילה וגם יקרה, משום שהמכוניות של ימינו עושות שימוש במערכות מחשב שונות. אולם, ככל שמכוניות יתחברו ביניהן באמצעות מערכות תקשורת מתקדמות ורשתות כלי רכב, כך תגבר האפשרות להשתלטות נרחבת של האקרים עליהן. למעשה, פריצות בודדות של האקרים למכוניות הן אפשרות הקיימת כבר היום. לדוגמה, צמד האקרים הצליח להשתלט על מערכות ההיגוי, הבלמים והתאוצה של ג'יפ באמצעות מערכת Uconnect של הרכב. מערכת הבידור של הג'יפ הייתה מחוברת לבקורות ההיגוי והבלמים שלו באמצעות רשת המחשב המכונה "CAN bus".³⁹ במכונית אוטונומית יש יותר חיבורים עם העולם החיצוני ויותר בקרה ממוחשבת של מערכות הרכב מאשר בג'יפ שעבר השתלטות, וכך גדלה הפגיעות של כלי רכב מסוג זה. חברת "אובר" אף שכרה לאחרונה את שירותיהם של שני ההאקרים שפרצו לג'יפ במטרה לשפר את האבטחה של כלי הרכב שלה.⁴⁰

יצרני הרכב חייבים להגן בצורה פרו-אקטיבית על מכוניות אוטונומיות מפני השתלטות של האקרים על עדכוני תוכנה, חיישנים ורשתות תקשורת: ראשית, עדכוני תוכנה דרושים כדי שהמכונית האוטונומית תפעל ביעילות, אך הם מהווים גם נקודת תורפה מרכזית,⁴¹ ואם הם יותקנו בצורה מקוונת, המערכת תהיה נתונה לסיכון גבוה אף יותר;⁴² שנית, אפשר להערים על חיישני המכונית. אם החיישן מזהה בטעות הולך רגל על הכביש, המכונית תעצור במפתיע.⁴³ אפשר להטעות חיישני לידאר (Lidar) באמצעות לייזר שעולה בסך הכול שישים דולר,⁴⁴ וישנו גם סיכון שנהגים "יפרצו" למכוניות שלהם עצמם או למערכת של המכונית שלהם במטרה לשנות את אופן ההתנהגות של הרכב.⁴⁵ בעלים שיפרצו למכוניות של עצמם במטרה להגביר את שליטתם ברכב יסכנו את ביטחונם.⁴⁶ הסיכון יגבר כאשר נהג במכונית הפרוצה ימצא עצמו נוסע ליד מכונית רגילה, שנהגה מצפה שהמכונית שנפרצה תנהג בצורה מסוימת; לבסוף, העובדה שמכוניות אוטונומיות יהיו מקושרות אחת לשנייה באמצעות רשתות תקשורת, תיצור נקודות פגיעות נוספות. מתקפות על מערכות "רכב לרכב", "רכב לתשתית" ו-GPS עלולות לפגוע בבטיחות, ב"הסכמת המשתמש" ובפרטיות.⁴⁷ תקשורת "רכב לרכב" פגיעה הן למתקפות מסוג של גניבת נתונים מרשת המחשב (CNE) והן למתקפות של השתלטות על רשת המחשב (CNA). מתקפת CNE כנגד תקשורת של מכונית אוטונומית עלולה לפגוע בפרטיותו של קורבן המתקפה,⁴⁸ שכן הנתונים של נסיעת הנהג המסוים יכולים לשמש נגדו. מתקפת CNA נגד מכונית אוטונומית יכולה

ליצור פעילות לא חוקית מזויפת ולדווח עליה, ובכך לגרום להשלכות לא נעימות לנהג.⁴⁹ האקרים שיפרצו לתקשורת "רכב לרכב" יכולים לשים את ידם על מפתחות, תוכנה, חיישנים ותשדורות יוצאות.⁵⁰ מתקפות DoS עלולות ליצור עומס יתר של מידע על המכונית, או לחילופין למנוע ממנה לשלוח מידע.⁵¹ Lacey מזהה שלושה סוגים של מתקפות נגד תקשורת מסוג "רכב לרכב" ו"רכב לתשתית". האקר יכול להשתמש ב"קישור הודעות" ולעקוב אחר "הודעת בטיחות בסיסית" של "רכב לרכב" כדי לגלות את מיקום המכונית. ב"מתקפת הפללה", ההאקר גונב תחילה את האישור המקוון של המכונית, ולאחר מכן שולח הודעות מזויפות שמעידות על נהיגה לא חוקית לכאורה. "מתקפת הפללה" עלולה לגרום למאסרו של נהג חף מפשע. ב"מתקפת סיביל", האקר גונב אישורים של מכוניות רבות, ולאחר מכן שולח הודעות מכל אחת מהן שמצביעות על נהיגה לא חוקית של מכונית מסוימת.⁵² "מתקפת סיביל" עלולה גם היא להפליל נהג המציית לחוק. כל אחת מפגיעויות אלו מהווה מכשול במרוץ לפיתוח מכונית אוטונומית בטוחה. ככל שהיצרנים וחברות הטכנולוגיה ימציאו פתרונות חדשים לאותן פגיעויות, כך הם יתקרבו למטרה שהציבו לעצמם.

מניעים להשתלטות של האקרים

טרור הוא איום מרכזי על מכוניות אוטונומיות. דרך מצוינת לבצע פיגוע ראויה על ידי טרוריסט שיש לו מומחיות טכנית ושאיפות לפרסום בין-לאומי, היא השתלטות על מכונית אוטונומית אחת או יותר. אפילו השתלטות בקנה מידה קטן על כמה מכוניות בלבד עלולה להשבית את מערך התחבורה. מתקפה כזאת תזרע חשש בקרב הנוסעים במכוניות האוטונומיות ובכלי הרכב הרגילים גם יחד, משום שאם מכונית אוטונומית שהאקר הצליח להשתלט עליה נוסעת בכביש, אף מכונית לידה אינה בטוחה. חשש מפני מצב כזה עלול להביא לירידה כוללת בשימוש במכוניות, וכתוצאה מכך לקריסה של הכלכלה האמריקאית. לדוגמה, לאחר מתקפות הטרור על ארצות הברית ב־11 בספטמבר 2001, מספר הטסים במטוסים שם ירד באופן דרמטי ולא חזר לעצמו עד 2004.⁵³ מכוניות אוטונומיות יכולות לשמש טרוריסטים גם כדי לפגוע במטרות ספציפיות. מתקפה על מכונית יחידה, שתהיה מוסוית היטב, אף עשויה להיראות כמו כשל טכני.

האקרים יכולים לנסות לפגוע במכונית אוטונומית גם כדי לסחוט צרכנים או אפילו את ממשלת ארצות הברית. אם צרכן מקבל הודעה מהמכונית שלו שהיא תבצע תאונה מכוונת, אלא אם יועבר כסף לחשבון מקוון כלשהו, אותו צרכן ייאלץ, קרוב לוודאי, לציית לדרישה. באופן דומה, ארגון פשע יכול להודיע לממשלת ארצות הברית כי השתלט על כמה מכוניות לא מזוהות, ואז לאלץ אותה להיענות לדרישותיו, שאם לא כן יפתח הארגון במתקפה מסיבית. למרבה המזל, האקר

שהמניע שלו הוא כספי יגלה שהתהליך של השתלטות על מכונות אוטונומיות יקר למדי.⁵⁴ השתלטות על מכונות אוטונומיות תהיה אטרקטיבית רק אם האקרים יגלו דרך להרוויח מכך כסף.⁵⁵ בנוסף, כפי שציין אחד ההאקרים המזהה עצמו כ"כובע לבן", אנשים שיש להם את הידע הטכני הדרוש כדי להשתלט על מערכות תקשורת של מכונות, בדרך כלל לא רוצים להרוג אנשים אחרים.⁵⁶ סיכון חמור יותר הוא סחיטה פוליטית. למשל ארגון "אנונימוס", יכול להשתלט על מכונות אוטונומיות כדי לתבוע מממשלת ארצות הברית לשנות מדיניות מסוימת.

ממשלות זרות הן איום פחות חמור מאשר טרוריסטים ופושעים. הן יכולות לכוון לפגיעה ברשת תקשורת של מכונות אוטונומיות, אולם סביר להניח שהשיבושים שייגרמו כתוצאה מכך בכלכלה האמריקאית ישפיעו גם על אותן ממשלות עצמן. עם זאת, קשה לסמוך על כך שממשלות זרות אכן יפעלו על פי שיקול זה.

פתרונות אפשריים

כדי לצמצם את הסיכוי למתקפות סייבר על מכונות אוטונומיות, חיוני לאבטח את תשתית הענן, להגן על הטלקומוניקציה ולבחון את הפגיעויות הספציפיות של מכונות אוטונומיות. יש שורה של פתרונות טכניים ומשפטיים לפגיעויות האופייניות למכונות כאלו.

כאמור, הגנה על תשתית הענן מפני מתקפות סייבר חיונית לצורך אבטחת המכונות האוטונומיות. חברות הטכנולוגיה צריכות להיצמד ל"שיטות עבודה מומלצות לאבטחת יישומים", וכך הן יוכלו לקבל גישה לרשת כדי לאבטח את הענן.⁵⁷ נוהלי דיווח ובדיקות מחמירים יסייעו גם הם לוודא קיומה של רשת מאובטחת.⁵⁸ ולבסוף, צוותי אבטחת הסייבר חייבים לפעול כמו מכבי אש, ולהיות מוכנים להגיב במהירות למתקפות סייבר.⁵⁹

הגנה על הטלקומוניקציה, לרבות תקשורת "רכב לרכב" ו"רכב לתשתית", חיונית לשמירה על הפרטיות והביטחון. חינוך, שיתוף פעולה שמכבד זכות לפרטיות, חוקים ומנהיגות יכולים לסייע להגן על תשתית הטלקומוניקציה מפני מתקפות סייבר.⁶⁰ כדי להשיג תקשורת יעילה של "רכב לרכב" ו"רכב לתשתית", המכונות צריכות לשדר הודעות בטיחות בסיסיות חד-סטוריות ולא מוצפנות, שיהיו זמינות לקריאה על ידי כלי הרכב הסמוכים, וזאת בנוסף לתקשורת מאובטחת ואמינות מוצפנות.⁶¹ לדוגמה, חברת הזנק ישראלית בשם "ארגוס" מפתחת דרך שמאפשרת לקבוע אילו הודעות הן חוקיות ואילו זדוניות.⁶²

יש גם פתרונות אפשריים ספציפיים למכונות אוטונומיות. פתרונות אלה, כאשר הם ישולבו ביחד, יפחיתו את הסיכוי להצלחתה של מתקפה על הרכב האוטונומי. לצורך זה יש לנקוט את הפעולות הבאות: ראשית, על המפתחים להכיר היטב את דפוסי התנועה והדרך שבה מכונות אוטונומיות מתקשרות עם מכונות אחרות, עם

רוכבי אופניים ועם הולכי רגל. הבנה כזאת תאפשר להם להבחין בין התנהגות נהיגה רגילה לבין התנהגות נהיגה שנתונה להשתלטות עוינת.

שנית, על מפתחי המכוניות האוטונומיות להבטיח אפשרות של זיהוי חיובי של מכונית ספציפית כזו או של מקור העדכון של התוכנה שלה. "תשתית מפתחות ציבוריים" (Public Key Infrastructure – PKI) יכולה לנהל את אישורי הזיהוי של המכוניות האוטונומיות באופן מקוון,⁶³ בעוד ש"רשות אישורים" תהיה אחראית להקצאת אישורים מקוונים למכוניות כאלו.⁶⁴ המערכת שתקצה אישורים מסוג זה תוכל להיות "ממורכת, מבוזרת או היברידית",⁶⁵ והאישורים עצמם יזהו מכוניות שמשתייכות למערכת זאת.⁶⁶ בשלב הבא, חברות יתבקשו להבטיח שהמכוניות יוכלו לזהות עדכוני תוכנה חוקיים. מכוניות אוטונומיות יהיו מסוגלות להבחין בין עדכוני תוכנה חוקיים למזויפים באמצעות מנגנוני "לחיצת יד" (handshake).⁶⁷ יש גם שורה של פתרונות טכניים שיאפשרו למערכות המחשב של המכוניות האוטונומיות לוודא שהן מחוברות למכונית הנכונה וכי הן מריצות תוכנה חוקית.⁶⁸ "בדיקות סבירות" יגבילו את התוכנה שניתן להפעיל על יחידת הבקרה האלקטרונית (ECU) של המכונית,⁶⁹ ו"זיהוי רכיב" יוצמד ליחידת הבקרה האלקטרונית.⁷⁰ חלק נוסף של התוכנה ינסה לזהות נתונים חריגים.⁷¹

שלישית, מפתחי מכוניות אוטונומיות צריכים להפריד בין מערכות מחשב חיוניות לבלתי חיוניות. השתלטות ההאקרים על הג'יפ, שתוארה לעיל, ממחישה את הפגיעות של מכוניות שהפונקציות שלהן מקושרות כולן בצורה אלקטרונית. Camek ואחרים ממליצים שיצרני הרכב יבנו מכוניות עם "שכבות אבטחה מרובות ובלתי תלויות" (MILS), שיש להן יכולות "מסתגלות" ו"מבוזרות".⁷² ארכיטקטורת MILS בונה מחסום בין מחשבים חיוניים למחשבים לא חיוניים במכונית. ההפרדה בין מערכות המחשב יכולה למנוע מווירוס להגיע לפונקציות חיוניות ברכב.⁷³ מערכת מבוזרת תאפשר לארכיטקטורת MILS לפעול על מספר רב של מחשבים. מערכת מסתגלת תאפשר עדכון של יכולות חדשות.⁷⁴ מרכיבים אלה יסייעו לצמצם את הסיכוי של מתקפה על מכוניות אוטונומיות בעתיד.

רביעית, יצרנים צריכים לחפש אחר פתרונות טכניים נוספים. "קופסאות שחורות", שבמקור הן משמשות במטוסים, יוכלו להקליט נתונים על תאונות מבלי שיקליטו בהכרח נתוני GPS פרטיים.⁷⁵ נתונים אלה יוכלו לשמש ללימוד הטעויות שהובילו לתאונה ולספק רמזים לשאלה אם הייתה השתלטות על כלי הרכב. יש לצייד מכוניות אוטונומיות גם ב"מצב בטוח", שיאפשר להשבית את התכונות האוטונומיות שלהן,⁷⁶ כך שבמקרה של השתלטות, הנהג יוכל להחזיר לעצמו בביטחה את השליטה על הרכב. כדי לאפשר "מצב בטוח", יהיה צורך לשמר במכונית האוטונומית את ההגה המסורתית ואת דוושת הבלמים. יצרנים יידרשו גם להיצמד לתקני התעשייה ולבדיקות מקיפות של כלי הרכב.⁷⁷

חמישית, לצד המאמצים הרבים להגנה על רכב אוטונומי מפני אתגרים טכניים, חשוב גם לבחון פתרונות משפטיים. חוקים נכונים יכולים הן להרתיע האקרים והן להקשות עליהם בניסיונותיהם להשתלטות עוינת. ואמנם, מדינות שונות כבר מיישמות חוקים בנוגע לבדיקת מכוניות אוטונומיות.⁷⁸ על המדינות לפעול ליישום חוקים המחייבים יצרני מכוניות אוטונומיות להיצמד לשיטות עבודה מומלצות בכל הנוגע לאבטחה. המחוקק המקומי והממשלתי גם יכול ליזום חקיקה שתגן על רישיונות. מכיוון שבלתי אפשרי לתכנן מכונית שהחומרה שלה חסינה באופן מוחלט מפני פריצות, החוק יצטרך להרתיע אנשים שהשיגו גישה פיזית לרכב מגניבת מפתחות תוכנה.⁷⁹ בנוסף, ניתן לעשות שימוש בחוקים המגנים על מערכות אוטונומיות קיימות, כגון אלו המשמשות במערכות בקרה אוויריות. ניתן להרחיב חוקים אלה כך שיכסו גם מכוניות אוטונומיות, ככל שאלו יהפכו לנפוצות יותר. שיטית, גם חברות פרטיות ובתי המשפט יכולים למלא תפקיד במציאת פתרונות אפשריים לפגיעויות של כלי רכב אוטונומיים. בתי המשפט חייבים לקבוע כיצד להגיב לתאונות שנגרמו בעקבות השתלטות של האקרים. חברות שאוספות נתונים על מכוניות אוטונומיות צריכות לשאת באחריות משפטית להגנה על נתונים אלה.⁸⁰ דרישות מסוג זה יעודדו אותן חברות להשקיע באבטחת נתונים.

דילמות אתיות

מכוניות אוטונומיות משתמשות בתשתית ענן במצבים שיש להם נגיעה לחיים ומוות, ולכן הן מעלות שאלות אתיות רבות. אמנם, אין מקום לדיון אתי מפורט במאמר זה, אך בכל זאת כדאי לסקור כמה מהשאלות הנפוצות המופיעות בספרות בסוגיה זאת. מערכות אתיקה יכולות להתמקד בתועלתנות, זכויות, צדק, "הטוב המשותף" או תכונות טובות.⁸¹ אפתח בגישה התועלתנית, שכן המכוניות האוטונומיות מבקשות להציל כמה שיותר חיי אדם, או כפי שציין אלכסנדר קוט (Kott): "מכוניות ללא נהג יהרגו אנשים, אבל פחות".⁸² מנקודת מבט תועלתנית, הבחירה המתבקשת היא, אפוא, לעשות שימוש במכוניות אוטונומיות. Turck הולך צעד נוסף קדימה וטוען כי מכונית אוטונומית צריכה להיות מתוכנתת לא רק להצלת חיים, אלא גם כדי לשמור שהתנועה של מיליוני נהגים תזרום ללא הפרעה.⁸³ מכיוון שהאלגוריתמים של המכוניות האוטונומיות נכתבים מראש, כל שינוי הנוגע לחיים ולעניינים שבנוחות נקבע גם הוא מראש. כאשר המתכנתים מקודדים את האלגוריתמים של המכונית, עליהם לדאוג שאלה יהיו "עקביים", להימנע מלעורר "זעם ציבורי" ו"לא לרפות את ידי הרוכשים".⁸⁴ יצרני המכוניות האוטונומיות גם יצטרכו לבחור בין הרג של הולך רגל ובין הריגת הנהג. Frowe טוען שבעצם הבחירה להיכנס לכלי הרכב, הנהג מקבל על עצמו אחריות, ולכן הוא צריך להסתכן בכך שחיי הולך הרגל יקבלו עדיפות גבוהה יותר על חייו שלו.⁸⁵ במקרה

כזה יהיה צורך בפסיכולוגים ובנתוני סקרים כדי לבנות אלגוריתמים קבילים, שכן אנשים עשויים להסתייג מלהיכנס למכונית אוטונומית "תועלתנית" שתבחר להרוג אותם ולהציל את הולך הרגל.⁸⁶ העקביות באלגוריתמים חיוניות גם היא. אחרת תיתכן אפליה כלכלית, שכן אלה המסוגלים להרשות לעצמם לרכוש רכב שיגן על הנהג בוודאי יעשו זאת.

אתגר נוסף שיש לבחון הוא מי אחראי לתאונה. ככל שהמכונית האוטונומית תהפוך לנפוצה יותר, כך יהיה צורך לקבוע מי אחראי לתאונות – היצרנים או האדם היושב ברכב.⁸⁷ התשובה יכולה להיות תלויה בשאלה אם המכונית היא אוטונומית (רמה 3) או ללא נהג (רמה 4). לבסוף, ישנה הסוגיה של רשת כלי רכב אוטונומיים הנוטלים את חופש הבחירה מהאדם: ממשלה השולטת ברשת יכולה לקבוע לא רק את מהירות הנהיגה של כלי רכב אוטונומיים, אלא גם את יעדיהם. רשת כזאת יכולה, לפיכך, לאפשר לממשלה לשלוט בניידותם של בני אדם.⁸⁸

השלכות ונושאים למחקר נוסף

האם כל מה שנכתב לעיל מוביל למסקנה שיצרני הרכב האוטונומי צריכים "להרים ידיים"? האם האתגרים הטכניים והבטיחותיים הייחודיים של רכב מסוג זה הם כה גדולים, עד שחברות הטכנולוגיה והיצרנים צריכים להקפיא את פיתוח המכונית האוטונומית עד שתהיה בטוחה יותר? התשובה לשאלות אלו היא שלילית לחלוטין. מפתחי המכונית האוטונומית צריכים להמשיך בהתקדמותם, משום שמכוניות אוטונומיות, על כל הליקויים הנוכחיים שקיימים בהן, יכולות למנוע תאונות ולהציל חיים. אלון מאסק, מייסד "טסלה", התייחס לכך לאחרונה, כשכתב כי החברה שלו אינה מתעכבת במאמציה להוציא לשוק מכוניות אוטונומיות, משום ש"כאשר נעשה שימוש נכון [במכונית אוטונומית, היא תהיה] בטוחה משמעותית יותר מאשר אדם הנוהג בעצמו, ולכן תהיה זו שגיאה מוסרית לעכב את יציאתה לשוק רק בשל החשש מפרסום שלילי או חישוב מסחרי כזה או אחר הנוגע לאחריות משפטית".⁸⁹ במקביל לפיתוח המכונית האוטונומית, חייבים המתכננים להמשיך ולפתח אמצעי בטיחות יעילים יותר.

למכונית האוטונומית יש השלכות רבות שיכולות להוביל למחקרים נוספים. השלכות אלו כוללות, בין השאר, את המחלוקת סביב הזכות להשתמש בתקשורת ייעודית אלחוטית לטווח קצר (DSRC),⁹⁰ אבטחת סייבר של כטב"מים,⁹¹ התאמת המכונית האוטונומית להתנהגות הבלתי מושלמת של הנהג האנושי,⁹² והצמיחה של תעשיית הבידור הקשורה למכוניות. חששות משפטיים שיש לחקור את משמעויותיהם והשלכותיהם כוללים את האחריות על תאונות,⁹³ את החוקיות של שירותי מעקב משטרה כגון אלה שמציעה תוכנת "ווייז", ההשפעה של המכונית

האוטונומית על חברות הביטוח, והסיכון מהפעלת מניפולציה על נתוני המכונית כדי ליצור מצג שווא.

כך או כך, כדאי שנהדק את חגורות המושב בעודנו מאיצים את מכוניותינו לעבר עולם האינטרנט של הדברים.

הערות

- 1 Isaac Asimov, "Sally", in Nightfall Two (Frogmore: Granada, 1976).
- 2 James M. Anderson, Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras and Oluwatobi A. Oluwatola, Autonomous Vehicle Technology: A Guide for Policymakers (Santa Monica: RAND, 2014), p. 66.
- 3 "Why Autonomous and Self-Driving Cars Are Not the same", Economist, July 1, 2015, <http://www.economist.com/blogs/economist-explains/2015/07/economist-explains>.
- 4 Elon Musk, "Master Plan Part Deux", Tesla (blog), July 20, 2016, <https://www.tesla.com/blog/master-plan-part-deux>.
- 5 "U.S. Department of Transportation Releases Policy on Automated Vehicle Development", NHTSA, May 30, 2013, <http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development>.
- 6 שם.
- 7 Anderson and others, Autonomous Vehicle Technology, p. 60.
- 8 שם, עמ' 61.
- 9 שם, עמ' 61-62.
- 10 שם.
- 11 שם, עמ' 62.
- 12 שם, עמ' 64.
- 13 "How Does a Self-Driving Car Work?", Economist, April 29, 2013, <http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-self-driving-car-works-driverless?fsrc=scn/fb/wl/bl/tr/st/howdoesaself-drivingcarwork>.
- 14 Anderson and others, Autonomous Vehicle Technology, p. 64.
- 15 "How Does a Self-Driving Car Work?"
- 16 Christoph Ponikwar and Hans-Joachim Hof, "Overview on Security Approaches in Intelligent Transportation Systems: Searching for Hybrid Trust Establishment Solutions for VANETs", Secureware (2015): The Ninth International Conference on Emerging Security Information, Systems and Technologies, eds. Rainer Falk, Carla Merkle Westphall and Hans-Joachim Hof (Wilmington, DE: IARIA, 2015), <http://toc.proceedings.com/27725webtoc.pdf>.
- 17 שם, עמ' 1.
- 18 Anderson and others, Autonomous Vehicle Technology, p. 80.
- 19 Douglas Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems: Development, Challenges and Security Proposals (New York: Nova Science, 2014), p. 10.

- “Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Development Challenges Exist”, United States Government Accountability Office (2013). 20
- Anderson and others, *Autonomous Vehicle Technology*, p. 58. 21
- Jerry L. Archer, “International Engagement on Cyber V: Securing Critical Infrastructure”, *Georgetown Journal of International Affairs* (2015): 168. 22
- Andreas Riener, “Who Cares about Trust, Grade of Traveling and Quality of User Experience in a World of Autonomous Cars?”, *AutomotiveUI ‘14, Adjunct Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications* (2014): 1-3. 23
- Nick Lavars, “Self-driving Truck Hits the Highway in World First”, *New Atlas*, October 4, 2015, <http://newatlas.com/daimlers-production-autonomous-truck-debuts-public-roads/39701/>; David Sedgwick, “Army Eyes Self-Driving Convoys”, *Automotive News*, August 4, 2015, <https://www.autonews.com/article/20150804/OEM06/308059984/army-eyes-self-driving-convoys>. 24
- Benjamin Snyder, “Tesla CEO Elon Musk just told us When all Cars will be Self-Driving”, *Fortune*, November 4, 2015, <http://fortune.com/2015/11/04/tesla-elon-musk-self-driving-cars/>. 25
- “Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Development Challenges Exist”, p. 7. 26
- “Upsetting the Apple Car”, *Economist*, February 21, 2015, <http://www.economist.com/news/business/21644149-established-carmakers-not-tech-firms-will-win-race-build-vehicles>. 27
- Nikhil Gowda, Wendy Ju and Kirsten Kohler, “Dashboard Design for an Autonomous Car”, *AutomotiveUI ‘14, Adjunct Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications* (2014): 1-4. 28
- “Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Development Challenges Exist”, p. 8. 29
- Lacey, *Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems*, p. 25. 30
- Anderson and others, *Autonomous Vehicle Technology*, pp. 15-16. 31
- “How Autonomous Vehicles will Shape the Future of Surface Transportation”, United States Subcommittee on Highways and Transit (2013), p. vii. 32
- שם. 33
- שם, עמ' 7. 34
- The Tesla Team, “A Tragic Loss”, *Tesla (blog)*, June 30, 2016, <https://www.tesla.com/blog/tragic-loss>. 35
- שם. 36
- Anderson and others, *Autonomous Vehicle Technology*, p. 9. 37
- שם, עמ' xvii. 38
- Andy Greenberg, “Hackers Remotely Kill a Jeep on the Highway – With Me in It”, *Wired*, July 21, 2015, <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>. 39

- Roberto Baldwin, "Jeep Hackers Get New Jobs at Uber's Autonomous-car Lab", 40
Egadget, August 28, 2015, <https://www.engadget.com/2015/08/28/uber-jeep-hackers/>.
- Anderson and others, Autonomous Vehicle Technology, p. 70. 41
שם. 42
- שם, עמ' 71. 43
- Anna Peel, "Self-Driving Cars Can Be Disabled with Lasers", ValueWalk, 44
September 8, 2015, <http://www.valuwalk.com/2015/09/self-driving-cars-can-be-disabled-with-lasers/>.
- Anderson and others, Autonomous Vehicle Technology, p. 71. 45
שם. 46
- Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems, p. 47
54.
- שם, עמ' 72. 48
- שם. 49
- שם, עמ' 68-69. 50
- שם, עמ' 69. 51
- שם, עמ' 72-73. 52
- "Airline Travel Since 9/11", United States Department of Transportation, Bureau 53
of Transportation Statistics Issue Brief, no. 13, December 2005, http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/special_reports_and_issue_briefs/issue_briefs/number_13/html/entire.html.
- James Guy and Mat Greenfield, "Can Driverless Cars Ever Be Made Hack- 54
Proof?", The Guardian, March 9, 2015, <https://www.theguardian.com/technology/2015/mar/09/driverless-cars-safe-hackers-google>.
- שם. 55
- שם. 56
- Jerry L. Archer, "Dynamic and Effective Security in the Rapidly Evolving Global 57
Cloud Computing Cyberspace", Georgetown Journal of International Affairs
(2015): 173.
- שם, עמ' 174. 58
- שם, עמ' 175. 59
- Tarek Saadawi and Haidar Chamas, "Securing Telecommunications Infrastructure 60
against Cyber Attacks", Georgetown Journal of International Affairs (2015): 58-
69.
- Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems, p. 61
64.
- Kobe Liani, "Israeli Start-Up Will Protect your Car [from] Cyber Terrorism", 62
Walla, March 23, 2015, <http://cars.walla.co.il/item/2839940>.
- Lacey, Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems, p. 63
63.
- שם, עמ' 81. 64
- Ponikwar and Hof, "Overview on Security Approaches in Intelligent 65
Transportation Systems: Searching for Hybrid Trust Establishment Solutions for
VANETs", pp. 160-165.

- שם. 66
- Anderson and others, *Autonomous Vehicle Technology*, p. 70. 67
- Lacey, *Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems*, p. 68
- 79.
- שם, עמ' 78. 69
- שם, עמ' 79. 70
- שם. 71
- Alexander Georg Camek, Christian Buckl and Alois Knoll, "Future Cars: 72
- Necessity for an Adaptive and Distributed Multiple Independent Levels of
- Security Architecture", *HiCoNS '13, Proceedings of the 2nd ACM International*
- Conference on High Confidence Networked Systems (2013)*: 17-24.
- "Five Star Automotive Cyber Safety Program", *I Am the Cavalry*, February 2015, 73
- <https://www.iamthecavalry.org/domains/automotive/5star/>.
- Camek and others, "Future Cars: Necessity for an Adaptive and Distributed 74
- Multiple Independent Levels of Security Architecture".
- "Five Star Automotive Cyber Safety Program". 75
- שם. 76
- שם. 77
- Anderson and others, *Autonomous Vehicle Technology*, pp. 41-52. 78
- Lacey, *Vehicle-to-Vehicle Technologies for Intelligent Transportation Systems*, p. 79
- 77.
- Archer, "International Engagement on Cyber V: Securing Critical Infrastructure", 80
- p. 174.
- Manuel Velasquez, Dennis Moberg, Michael J. Meyer, Thomas Shanks, Margaret 81
- R. McLean, David DeCosse, Claire André and Kirk O. Hanson, "A Framework
- for Thinking Ethically", *Markkula Center for Applied Ethics*, August 1,
- 2015, [https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/a-](https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/a-framework-for-ethical-decision-making/)
- [framework-for-ethical-decision-making/](https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/a-framework-for-ethical-decision-making/).
- Alexander Kott, *Cybersecurity*, Lecture at Georgetown University, Washington, 82
- D.C., 2015. (צריך להוסיף כותרת ההרצאה)
- Mitch Turck, "An Autonomous Car might Decide you should Die", *Backchannel*, 83
- March 10, 2015, [https://backchannel.com/reinventing-the-trolley-problem-](https://backchannel.com/reinventing-the-trolley-problem-85f3d1730756#.lnpj44f1l)
- [85f3d1730756#.lnpj44f1l](https://backchannel.com/reinventing-the-trolley-problem-85f3d1730756#.lnpj44f1l).
- Jean-François Bonnefon, Azim Shariff and Iyad Rahwan, "Autonomous 84
- Vehicles Need Experimental Ethics: Are We Ready for Utilitarian
- Cars?", *arXiv:1510.03346v.1 [cs.CY]*, October 12, 2015, [http://arxiv.org/](http://arxiv.org/pdf/1510.03346v1.pdf)
- [pdf/1510.03346v1.pdf](http://arxiv.org/pdf/1510.03346v1.pdf).
- Olivia Goldhill, "Should Driverless Cars Kill Their Own Passengers to Save a 85
- Pedestrian?", *Quartz*, November 1, 2015, [http://qz.com/536738/should-driverless-](http://qz.com/536738/should-driverless-cars-kill-their-own-passengers-to-save-a-pedestrian/)
- [cars-kill-their-own-passengers-to-save-a-pedestrian/](http://qz.com/536738/should-driverless-cars-kill-their-own-passengers-to-save-a-pedestrian/).
- Bonnefon and others, "Autonomous Vehicles Need Experimental Ethics". 86
- Alexander Hevelke and Julian Nida-Rümelin, "Responsibility for Crashes of 87
- Autonomous Vehicles: An Ethical Analysis", *Science and Engineering Ethics* 21,
- no. 3 (2015): 619-630.
- ראיון של המחבר עם, Fr. Dennis McManus, 8 בדצמבר 2015. 88

- Musk, "Master Plan Part Deux". 89
- Anderson and others, Autonomous Vehicle Technology, p. 80. 90
- Jon Fingas, "The U.S. Navy wants to Protect its Drones against Hacks", Egadget, 91
May 20, 2015, <https://www.engadget.com/2015/05/20/us-navy-wants-hack-resistant-drones/>.
- Matt Richtel and Conor Dougherty, "Google's Driverless Cars Run into Problem: 92
Cars with Drivers", The New York Times, September 1, 2015, http://www.nytimes.com/2015/09/02/technology/personaltech/google-says-its-not-the-driverless-cars-fault-its-other-drivers.html?_r=0.
- "Safer at any Speed?", Economist, March 3, 2012, <http://www.economist.com/node/21548992>. 93