תוכן

מבוא

עולמנו תלוי במידה רבה והולכת במחשבים המתקשרים זה עם זה. בכמעט כל ההיבטים של החיים המודרניים נעשה שימוש במחשבים המופעלים בבטחה, הפותרים בעיות גדולות וקטנות מחיזוי מזג האוויר ועד להפעלת רשתות החשמל. קשרים בין מחשבים מפעילים את רוב מעברי ההון והעסקאות הנעשות בעולם, גביית המסים, הפעלת עסקים ועוד. טכנולוגיית המחשבים היא אחת מהכלים החשובים ביותר שהומצאו אי פעם, והיא גרמה למהפכה בדרכים בהן חברות אנוש מתארגנות ומתנהלות. אין תחום חיים שהיא לא נוגעת בו, ולא ניתן להמעיט בחשיבותה והשפעתה (Newman, et al.,2018)

בימים הראשונים של מרחב הסייבר – העולם המקושר באמצעות מחשבים הפועלים על כוח חשמלי ומעבירים מידע המיועד לצריכה אנושית – הוא סיפק הזדמנויות ויתרונות רבים לחברה הדמוקרטית. זה נכון במיוחד בנוגע לפעולתן היעילה של ממשלות, לאפשרות שלהן לתקשר עם אזרחיהן וליכולתם של האזרחים לתקשר זה עם זה (Warren,2017). עם זאת, ההתפתחויות בשנים האחרונות במרחב הסייבר וביחסי הסייבר הבינלאומיים הולידו דאגות וחששות בקרב חוקרים, פוליטיקאים, אזרחים וגורמי ביטחון מפני ניצול מרחב זה לרעה לביצוע פשיעה, טרור ולצרכים פוליטיים.

בתקופה האחרונה, מתקפות סייבר על מדינות ועל מוסדות בינלאומיים נעשו יותר ויותר מתוחכמות ונועזות. הראיות מייחסות את מקורותיהם של מתקפות הסייבר האלו לארגוני פשע בינלאומיים, שחקנים בינלאומיים סוררים (כגון ארגוני טרור) ובמיוחד למדינות זרות אשר בגלוי ובחשאי הובילו מתקפות מתואמות וקמפיינים של תעמולה במטרה לערער ולהשפיע על היבטים שונים של הדמוקרטיה.

מדינות דמוקרטיות הן פגיעות במיוחד – הרבה יותר ממדינות לא דמוקרטיות, כפי שיוסבר בהמשך – להתקפות סייבר המכוונות להשפיע על השיח, המוסדות, והתהליכים אשר מתקיימים בהן. בחלקו הדבר נובע ממאפייניהן הייחודיים הנגזרים מהגדרת הדמוקרטיה, ובחלקו ממאפיינים המתקיימים בהן בפועל. ראשית, מדינות דמוקרטיות מכירות בכל אזרחיהן כשווים, וכזכאים באופן שווה להביע את קולם ולהשפיע על התהליכים הפוליטיים שבהן. שנית, אזרחיהן של מדינות דמוקרטיות מנסחים לעצמם את סדר היום וההעדפות שלהם בנוגע למדיניות אותה יש לנקוט בתחומים שונים. העדפות אלה מיתרגמות למדיניות משותפת שכולם יכולים לחיות עימה. זה מתבצע באמצעות מסגרות מוסדיות בהן מתקיים משא ומתן על החוקים והמדיניות. שלישית, מדינות דמוקרטיות ממסדות את ההוצאה לפועל הלגיטימית של רצון הציבור (Warren, 2017).

תפקידן המכריע של הרשתות החברתיות במדינות דמוקרטיות בולט במיוחד כשמעמידים אותו מול תפקודן במדינות בלתי דמוקרטיות. ניתן את איראן כדוגמא משמעותית ובולטת. משקיפים מערביים מדברים לעתים על "המדיה החברתית הפורחת באיראן" כדוגמא לכך שלמדיה זו יש שם תפקיד חברתי דומה לזה שבמדינות דמוקרטיות השומרות על חופש הביטוי וההבעה. הדימוי – השגוי לחלוטין – נובע כנראה מהכתרתן של מחאות 2009 באיראן כ"מהפכת הטוויטר" – שלא הצליחה באמת להביא מהפכה שתפיל את המשטר התיאוקרטי (Ali and Fahmy, 2013). אולם גם ב'מהפכת הטוויטר', שימוש מרכזי במדיה החברתית נעשה דווקא על ידי השלטון עצמו על מנת לעקוב אחר פעולות המפגינים, להתחקות אחר פעילי הרשת הבולטים ולהפסיק את פעולתם באיומים. יתר על כן, ההערכות הן כי הכינוי "מהפכת הטוויטר" הוא מוגזם וכי לרשת החברתית יוחס תפקיד גדול בהרבה מזה שהיה לה במציאות בארגון המחאות (Ali and Fahmy, 2013).

השלטון במדינה טוטליטרית כאיראן מסוגל להפעיל – ואכן מפעיל כל העת – אמצעים להגבלת המדיה החברתית אשר מונעים ממנה להשפיע על השיח במדינה, מוסדותיה והמדיניות הננקטת על ידי השלטונות בה. באיראן, הרשתות החברתיות המובילות Facebook ו- Twitter חסומות לחלוטין על ידי השלטונות מפני אזרחי המדינה, מאז 2009 (Kertscher, 2020). מגבלות על רשתות נוספות מושמות ומורדות בהתאם לצרכי ושיקולי הרשויות, באופן קבוע (Frenkel, 2018).

בימינו, חלק ניכר (אם לא כל) מהפעילויות החברתיות, השיח הציבורי והפעילות הפוליטית במדינות דמוקרטיות מתקיימים במרחב הסייבר. כל מרחב פעילות המתקיים ברשת האינטרנט מהווה למעשה הזדמנות למתקפת סייבר.

עבודה זו מתמקדת בסוג מסוים של מתקפות סייבר: מתקפות מידע וחברה (Information-Social Cyber Attacks) על המצביעים, המועמדים והמוסדות הדמוקרטיים במדינות נאט"ו (NATO). המתקפות שייבחנו בעבודה בוצעו בשנים האחרונות על ידי המודיעין של רוסיה על שתי מדינות נאט"ו- בריטניה וארצות הברית.

מטרתה של הברית הצפון-אטלנטית היא להבטיח את ביטחונן של המדינות החברות בה ואת החירויות הדמוקרטיות מפני תוקפנות חיצונית באמצעים פוליטיים וצבאיים (NATO, 1949), בזמן המלחמה מפני מדינות הגוש הסובייטי וכיום, בין השאר, מפני רוסיה. בנוסף, המדינה המובילה בנאט"ו, ארצות הברית, היא המקור למחקר המדעי ולפרויקטים שיצרו את מה שהפך להיות האינטרנט, ומאוחר יותר המרחב הקיברנטי. מדינות נאט"ו (לצד מדינות המערב הדמוקרטיות שאינן חברות נאט"ו) הן גם המובילות בשימוש במרחב הסייבר, כשבין 80% ל- 100% מהאוכלוסייה מחוברים לאינטרנט, ורובם משתמשים באופן פעיל ברשתות החברתיות. זאת לעומת מדינות בלתי דמוקרטיות כגון רוסיה, סין ואיראן (פחות ממחצית מאוכלוסיית איראן מחוברת לאינטרנט, מה שמפריך עוד יותר את הדימוי על השפעת הרשת החברתית ה"פורחת" בה) (Internet Live Stats, 2016).

בשנים האחרונות מדינות דמוקרטיות דיווחו כי תשתיות חיוניות ופעולות קריטיות של המדינה הותקפו באמצעים דיגיטליים. עם הזמן דיווחים אלה נעשו תכופים יותר, מפורטים יותר ומגובים בראיות רבות יותר (Stoltenberg, 2017). כפי שנראה ונסביר במהלך עבודה זו, מתקפות סייבר על מדינות דמוקרטיות, בהן סוכנים של מדינות זרות התערבו בהצלחה בתהליכים הדמוקרטיים בעזרת שיטות קיברנטיות, הגיעו לשלב חדש אשר ניתן לראותו כמתקפה על הדמוקרטיה (Pamment et al., 2019).

<u>שאלת המחקר:</u> לאור האמור לעיל, מטרתה של עבודה זו הינה לענות על השאלה – מדוע וכיצד פועלות מדינות זרות באמצעות יכולות סייבר כדי להשפיע על תהליכים דמוקרטים במדינות זרות, ועד כמה המהלכים האלה מצליחים?

<u>שדה ושיטת המחקר:</u> העבודה תבחן את האיומים האחרונים במרחב הסייבר על מדינות נאט"ו הדמוקרטיות. מקרי הבוחן בהם אתמקד יהיו מתקפות סייבר שבוצעו על שתי מדינות חברות