המענה הבריטי לאיומים במרחב הסייבר

דניאל כהן

איום הסייבר נמצא כיום במקום גבוה בין הגורמים המהווים סיכון לאינטרסים ולביטחון הלאומי של מדינות. איום זה בא לידי ביטוי בשנים האחרונות בסדרה של מתקפות סייבר על מוסדות פוליטיים, מפלגות, ארגונים, מוסדות פיננסיים ותשתיות לאומיות קריטיות בכול רחבי העולם. בעתיד הקרוב צפויים סיכונים נוספים הנובעים מאיום הסייבר, במיוחד על המגזר האזרחי, שמקורם ב"אינטרנט של הדברים". סיכונים אלה הם תוצאה של העלייה במספר המכשירים המחוברים, שרובם אינם מאובטחים על ידי היצרנים או המשתמשים, וכן של העלייה במספר התקפות מניעת שירות, בשילוב סחיטה ודרישות כופר, על מערכות ציבוריות ופרטיות.
מאמר זה מתמקד בנעשה בתחום ביטחון הסייבר בבריטניה. הפערים המובנים בין מאפייני המגזר הפרטי הבריטי, הגמיש והדינמי, ובין צורכי מערכת הביטחון החשאית, הביורוקרטית והאיטית משבעה, הֻקשו על שיתופי פעולה בין תעשיית הסייבר בבריטניה ובין המערכת הביטחונית שם ועל שיתוף ידע חוצה מגזרים כנדרש היום. כמענה למצב זה, יושמו בשנים האחרונות בבריטניה תהליכים אסטרטגיים ממשלתיים לתמיכה בנושאי חדשנות וטכנולוגיה, בדגש על תעשייה עתירת ידע וביטחון סייבר. משרתם של תהליכים אלה הייתה להתמודד עם הדינמיות המשתנה של איומי הסייבר, תוך ניסיון לבניית גשר בין סוכנויות הביון והמודיעין הבריטיות ובין השוק הפרטי, כולל בנושאי הגנה, מחקר ופיתוח.

מילות מפתח: ביטחון סייבר, בריטניה, מחקר ופיתוח, הגנת סייבר, GCHQ, NCSC, הרתעה, שיתוף פעולה בין־לאומי.

דניאל כהן הינו חוקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון ובמרכז למחקר סייבר בינתחומי ע"ש בלווטניק, אוניברסיטת תל אביב.

מבוא

לבריטניה היסטוריה ארוכה של שימוש במדע ובטכנולוגיה לצורכי ביטחון לאומי, וממשלותיה שמרו לאורך השנים על אסטרטגיה ומדיניות ארוכות טווח לתמיכה בנושאי חדשנות, טכנולוגיה ותעשייה עתירת ידע. צוותי סיגינט שפעלו מטעם משרד המלחמה הבריטי עסקו מאז מלחמת העולם הראשונה ביירוט תשדורות של הגרמנים, תוך שיתוף ידע עם צוותים מקבילים מצרפת. פיצוח קודים ואיסוף מודיעין התרחבו מאוד בבריטניה במלחמת העולם השנייה, ובשנת 1945 שירתו בשירות מודיעין הסיגינט הבריטי בבלצ'לי פארק כ־10,000 עובדים.[1]

"מטה התקשורת הלאומי" הבריטי (Government Communications Headquarters – GCHQ) הוקם בזמן המלחמה הקרה, ומאז הוא הגוף האחראי על סיגינט וטכנולוגיה, סייבר ומשימות נוספות בתחום הביטחון הלאומי בבריטניה. במקביל הוא משמש כגוף המנחה את ארגוני הממשל וארגוני תשתיות קריטיות בנושאי אבטחת מערכות מידע. לצד מחלקות אופרטיביות שונות, פועלת ב־GCHQ מחלקת מחקר מתקדמת העוסקת במגוון נושאים, כמו ארכיטקטורת רשת, אבטחה, בלשנות, בינה מלאכותית, מכונות אוטונומית ועוד.

ה־GCHQ עמד בשנת 2013 במוקד דיון ציבורי, עם פרסום דוח הממונה על המודיעין מטעם ממשלת בריטניה ובו המלצות לרפורמות, לחוקים חדשים ולתהליכים הנדרשים כדי להסדיר את אפשרויות המעקב והציתות על ידי המודיעין והמשטרה הבריטיים. הדוח הדגיש את הצורך ביצירת גשר בין סוכנויות הביון הבריטיות ובין השוק הפרטי בנושאי הגנה, שיתוף ידע ומו"פ.[2]

כחלק מהשינוי המבני שנועד להקים יכולת לאומית להגנת סייבר במגזר האזרחי, הודיעה ממשלת בריטניה בנובמבר 2015 על הקמת "מרכז ביטחון הסייבר הלאומי" (National Cyber Security Centre – NCSC). המרכז יהיה כפוף ל־GCHQ, אך יישא באחריות מדינתית להגנת הסייבר לכלל החברה הבריטית ויהווה כתובת אחודה לייעוץ ולתמיכה לטובת המערכת הכלכלית, תוך שיתוף פעולה ישיר עם האקדמיה וגורמים בין־לאומיים. כוונת הממשלה הבריטית הייתה לאפשר למערכת הביטחונית העוסקת בהתמודדות עם איומי הסייבר להפוך לנגישה יותר ולבעלת יכולת לשתף פעולה עם המגזר הפרטי לטובת שיתוף ידע ומשאבים.[3]

---

1 ראו אתר Government Communications Headquarters (GCHQ), https://www.gchq-careers.co.uk/about-gchq.html.

2 Mark Waller, "Report of the Intelligence Services Commissioner for 2013", *Intelligence Services Commissioner*, June 26, 2014, http://intelligencecommissioner.com/docs/40707_HC304IntelligenceServicesCommissioner_Accessible.pdf.

3 "Progress and Research in Cybersecurity: Supporting a Resilient and Trustworthy System for the UK", *The Royal Society*, July 2016, p. 37, https://royalsociety.org/topics-policy/projects/cybersecurity-research/.

מימון ממשלתי בריטי למחקר ופיתוח טכנולוגי

בשלושת העשורים האחרונים הפחית הממשל הבריטי את השקעותיו במחקר ופיתוח. בשנת 2012, לדוגמה, היו ההשקעות במו"פ כ־1.72 אחוזים מהתל"ג הבריטי, לעומת כשני אחוזים מהתל"ג בסוף שנות השמונים של המאה העשרים. נתון זה גם נמוך מהממוצע במדינות האיחוד האירופי, שעמד בשנת 2012 על 2.06 אחוזים.[4] בשנת 2014 קבעה הממשלה הבריטית יעד של עלייה בהשקעה המדינתית במו"פ, לרמה של שלושה אחוזים מהתל"ג עד שנת 2020.[5]

מרבית ההשקעות בטכנולוגיה ובחדשנות בבריטניה מוקצות כיום לעידוד המגזר הפרטי ולא הציבורי. התקצוב הממשלתי למדע ולמחקר עומד על כ־4.6 מיליארד ליש"ט בשנה, ואינו כולל הקצאות ישירות למגזר הביטחוני (שבו חל קיצוץ בתקציב מאז שנת 2010). בין השנים 2010–2014 צמחו התעשיות הדיגיטליות בבריטניה בכ־32 אחוזים – מהר יותר מאשר המשק הבריטי – וההעסקה בתעשיות אלו גדלה ב־2.8 אחוזים – מהר יותר משאר מגזרי המשק. בשנת 2015 היו 86 אחוזים ממשקי הבית במדינה מחוברים לאינטרנט ו־76 אחוזים ערכו קניות באמצעותו. כ־56 אחוזים מאוכלוסיית הבוגרים אזרחי בריטניה השתמשו בשנת 2016 בבנק דיגיטלי. תעשיית הדיגיטל בבריטניה מהווה היום כשבעה אחוזים מהכלכלה הבריטית, ומעסיקה חמישה אחוזים מכוח העבודה.[6] למרות התגברות השימוש במרחב הדיגיטלי, המשק הבריטי סובל מעלייה באחוזי האבטלה של בעלי מקצועות טכנולוגיים, ולעומת זאת קיים מחסור באנשי מקצוע בתחום הסייבר.[7] פער זה זוהה על ידי הממשלה, ומטרתה כיום היא להעמיק את שיתוף הפעולה בין GCHQ ובין התעשייה הבריטית ולתרום לצמיחת שוק הסייבר. שוויו של שוק זה מוערך כיום בכ־22 מיליארד ליש"ט, אך רק שני מיליארד ליש"ט הם הכנסות מייצוא מוצרי סייבר.[8]

4 Charlie Edwards and Calum Jeffray, "The Future of Research and Development in the UK's Security and Intelligence Sector", *Occasional Paper*, *Royal United Services Institute*, March 2015, https://rusi.org/publication/occasional-papers/future-research-and-development-uk%E2%80%99s-security-and-intelligence-sector.

5 "Research and Development Funding for Science and Technology in the UK", *National Audit Office*, *Memorandum for the House of Commons Science and Technology Committee*, June 2013, p. 7.

6 "Internet Access – Households and Individuals: 2015", *Office for National Statistics*, http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06.

7 "Jammin' in the Capital", *The Economist*, June 21, 2014, http://www.economist.com/news/britain/21604591-londons-creative-talents-have-unleashed-wave-innovative-technology-firms-jammin.

8 שם.

הצורך ביצירת מערכת סביבתית יעילה, בה יפעלו במשולב הממשלה, מערכת הביטחון, האקדמיה, תעשיות וחברות הזנק במטרה לענות על צורכי הביטחון הגוברים בשל עליית האיומים במרחב הסייבר, הביא את ממשלת בריטניה לגבש בשנת 2011 אסטרטגיה לאומית לביטחון סייבר לשנים 2011–2016. במסגרת זו החליטה הממשלה על השקעה של 860 מיליון ליש"ט בפיתוח תוכנית ביטחון סייבר לאומית.

יישום האסטרטגיה החדשה בא לידי ביטוי בשלב הראשון בהקמת גופי הגנה בסייבר, כגון ה־CERT הלאומי, פלטפורמות לשיתוף ידע, עידוד מחקרי סייבר באקדמיה וחלוקת אחריות בין הגופים השונים האמונים על ביטחון סייבר. למרות מספר הצלחות, אסטרטגיה זו לא הצליחה להתגבר על הפערים המבניים הקיימים בין המגזר הפרטי הגמיש והדינמי ובין צורכי מערכת הביטחון החשאית, הביורוקרטית והאיטית מטבעה. חוסר השקיפות המערכתי גם הקשה על ייעול שיתופי הפעולה בין התעשייה ובין המערכת הביטחונית בבריטניה ועל שיתוף ידע חוצה מגזרים. רוב תקציב הסייבר הלאומי הבריטי הושקע בשנים אלו בפיתוח יכולות הגנת סייבר מדינתיות, כולל הפניית תקציבים לגופי אכיפת החוק הנלחמים בפשע מאורגן. תקציבים נמוכים באופן יחסי הופנו למגזר הפרטי, לאקדמיה ולמערכת החינוך.[9]

עדכון אסטרטגיית הסייבר הלאומית של בריטניה

"אסטרטגיית הביטחון הלאומי" (NSS) הבריטית, שפורסמה בשנת 2015, הגדירה את איום הסייבר כאיום ראשון במעלה וכסיכון ברמה עליונה לאינטרסים של בריטניה.[10] שנה לאחר מכן פורסמה אסטרטגיית הסייבר הלאומית של בריטניה לשנים 2016–2021. במסגרת זו הוגדר ביטחון הסייבר כ"הגנה על מערכות מידע (תוכנה, חומרה ותשתיות נלוות), המידע שנמצא על מערכות אלו והשירותים שהמערכות מספקות, מפני חדירה של גורמים לא מורשים, נזק או שימוש לא נכון, כולל נזק שנעשה בכוונה תחילה על ידי מפעיל מערכת, או לא בכוונה כתוצאה מאי־עמידה בתקנות אבטחה".[11]

---

9 כשלושה רבעים מתקציב הסייבר הלאומי לשנים 2011–2016, בגובה של 650 מיליון ליש"ט, הופנו ל־GCHQ ולסוכנויות ביטחון נוספות. ראו: "The UK Cyber Security Strategy: Landscape Review", *National Audit Office*, February 12, 2013, p. 16, https://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf.

10 "National Security Strategy and Strategic Defence and Security Review 2015", November 23, 2015, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

11 Cabinet Office, National security and intelligence, HM Treasury, and The Rt. Hon. Philip Hammond MP, "HM Government, National Cyber Security Strategy 2016-2021", p. 15.

אסטרטגיית הסייבר הלאומית זיהתה את האיומים העיקריים הבאים על מרחב הסייבר הבריטי:[12]

- **פשיעת סייבר**: פשעים מבוססי סייבר המתבצעים באמצעות השימוש בטכנולוגיית מידע ותקשורת (ICT), כאשר גם התוקף וגם הקורבן משתמשים בכלי ICT; פיתוח נוזקות לביצוע הונאות פיננסיות, פריצה, גניבה, שיבוש או מחיקת מידע; פשעים "מסורתיים" בהם נעזרים הפושעים במחשבים, ברשתות מחשבים או בכול סוג אחר של ICT (כגון גניבת מידע או הונאה); פשיעת סייבר מאורגנת על ידי ארגוני פשיעה, בדגש על ארגונים דוברי רוסית שמקורם במזרח אירופה.
- **מדינות וקבוצות בחסות מדינתית**: ניסיונות חוזרים ונשנים של גורמים להסתנן לרשתות מידע בריטיות במטרה להשיג יתרונות אסטרטגיים, פוליטיים, טכנולוגיים, מדיניים ומסחריים. האיומים העיקריים בהקשר זה הם כלפי גורמי ממשל, ביטחון, כלכלה, אנרגיה ותקשורת. רק למספר מדינות מצומצם יש יכולת להוות איום רציני על בריטניה, אך מדינות רבות נוספות נמצאות בתהליכי פיתוח (או רכישה) של כלי סייבר שיוכלו להוות איום עליה בעתיד הלא רחוק. בנוסף לקמפיינים של ריגול, קיים איום של נשק סייבר התקפי גם נגד תשתיות קריטיות.
- **טרור**: קבוצות טרור מנהלות פעילות במרחב הסייבר נגד מטרות בריטיות, למרות שהיכולות הטכניות שלהן הן נמוכות בשלב זה. אף על פי כן, גם תקיפה באמצעות כלים פשוטים היא בעלת פוטנציאל לנזק גדול. עיקר האיום מגיע מתקיפות להשחתת אתרים, הדלפת פרטים אישיים וכדומה. מטרת ארגוני הטרור היא השגת חשיפה ציבורית והרתעת הקורבנות. הצפי הוא לעלייה בתדירותן של תקיפות מסוג מניעת שירות והשחתת אתרים, ולצד זאת התגברות האיום של הפעלת אנשים מבפנים (Insider Threat).
- **האקטיביזם**: מדובר בקבוצות של האקטיביסטים, שתקיפותיהן העיקריות הן מסוג מניעת שירות והשחתת אתרים. אלו הן קבוצות מבוזרות, המכַוונות את תקיפותיהן לנושאים ממוקדים ובוחרות את קורבנותיהן בקפידה.
- **Script Kiddies**: מדובר לרוב ביחידים בעלי יכולות סייבר מוגבלות שמשתמשים בכלי תקיפה שפותחו על ידי אחרים. הם אינם בעלי פוטנציאל להוות איום רחב על הכלכלה והחברה, אך בעלי פוטנציאל לגרום לנזק משמעותי ליחיד או לארגון.

האסטרטגיה שפורסמה ב־2015 לא השיגה את היעד של הבטחת נכסיה הדיגיטליים של בריטניה. מצב זה הביא את ממשלת בריטניה לתובנה כי נדרשת השקעת משאבים רבים יותר כדי לעמוד מול הדינמיות המשתנה של האיומים, והוביל לניסוח החזון לשנת 2021, הנשען על תפיסה אסטרטגית לאומית לביטחון סייבר.

12 שם, עמ' 18.

תפיסה זו כוללת ארבעה מרכיבים עיקריים: הגנה, הרתעה, פיתוח ופעילות בין־לאומית, כמפורט להלן:[13]

- **הגנה**: התבססות על המשאבים הקיימים בבריטניה להגנה מפני איומי סייבר במטרה ליצור יכולת תגובה אפקטיבית לאירועים ולהבטיח את תקינות הרשתות ומערכות המידע. נקודת המוצא היא שיש להגיע ליעד שבו אזרחים, עסקים והשירות הציבורי יהיו בעלי ידע ויכולת להגן על עצמם מפני תקיפות סייבר. לצורך זה תמקד הממשלה את משאביה, ביחד עם אלה של התעשייה, לפיתוח וליישום הגנת סייבר אקטיבית שתצמצם עד למינימום את תקיפות הסייבר בשגרה, ובהן תקיפות דיוג, פילטור כתובות IP זדוניות וחסימה אקטיבית של פעילות זדונית.[14] היכולת המדינתית נגד צורות תקיפה בסיסיות אלו תשפר את יכולת ההתגוננות הבריטית מול רוב איומי הסייבר הידועים.
- **הרתעה**: ביצור מרחב הסייבר הבריטי מפני כל צורות של תוקפנות, תוך זיהוי ניסיונות תקיפה, הבנתם, חקירתם ושיבושם. בנוסף לכך, רדיפת התוקפים והעמדתם לדין, גם על ידי פעילות התקפית במרחב הסייבר. בריטניה תפעל להעברת מסרים ברורים לאויביה על התוצאות הצפויות של כל איום או ניסיון לפגוע באינטרסים שלה או של בעלות בריתה במרחב הסייבר.
- **פיתוח**: תמיכה בחדשנות ובצמיחה של תעשיית הסייבר הבריטית. מדובר, בין היתר, במחקר ופיתוח מדעיים; בהשקעה במשאבים אנושיים במגזר הציבורי והפרטי; בהשקעה בהכשרת חוקרים ומומחים לאיומי הסייבר העתידיים; בהשקעה במחקר בראייה ארוכת טווח במטרה לעודד פיתוח הון אנושי של אנשי אקדמיה בתחום הסייבר.
- **פעילות בין־לאומית**: העמקת שיתופי הפעולה הקיימים עם השותפים הבין־לאומיים הקרובים לבריטניה ויצירת שיתופי פעולה חדשים לבניית יכולות שיסייעו לאבטחת נכסי הממלכה ברחבי העולם. שיתופי פעולה אלה יושגו באמצעות הסכמים בילטרליים ומולטילטרליים ויכללו, בין השאר, את האיחוד האירופי, נאט"ו והאו"ם.

דוח משותף של "סוכנות הפשיעה הלאומית" (NCA) ושל "מרכז ביטחון הסייבר הלאומי" (NCSC), שפורסם במארס 2017, מדגיש את הצורך בשיתוף פעולה בין התעשייה, הממשלה וגורמי אכיפת החוק בבריטניה לנוכח התגברות איום הסייבר והשינויים המהירים המתרחשים בתחום זה. הדוח מתמקד בתהליך שבו גורמי

13 שם, עמ' 15.

14 על פי נתוני הממשלה, מאז יוני 2016 נבלמו בסה"כ 54,456 מתקפות סייבר מסוג דיוג והחדרת וירוסים לאתרים. כ־36 אחוזים ממתקפות אלו מקורן בכתובות IP בריטיות. מתוך שאר המתקפות, 64 אחוזים כוונו ספציפית נגד אתרי ממשלה ויועדו להשגת פרטים אישים של אזרחים מתוך מאגרי מידע ממשלתיים.

פשע לומדים את הדרכים בהן שחקנים מדינתיים תוקפים ארגונים כגון מוסדות פיננסיים; בסיכון הנובע מ"האינטרנט של הדברים" לאור העלייה בשיעור המכשירים המחוברים, שרובם אינם מאובטחים על ידי היצרנים או המשתמשים; וכן בעלייה במספר התקפות מניעת שירות בשילוב עם סחיטות ודרישות כופר.[15]

יישום האסטרטגיה הבריטית הלאומית במרחב הסייבר

כדי להשיג את היעדים שהוגדרו באסטרטגיית הסייבר הלאומית לשנים 2016–2021, החליטה ממשלת בריטניה בשנת 2016 על השקעת 1.9 מיליארד ליש"ט בביטחון סייבר. החלטה זו באה בעקבות סדרת מתקפות סייבר אסטרטגיות על מוסדות פוליטיים, מפלגות וגופים פרלמנטריים, וכן איסוף מידע על תשתיות בריטיות לאומיות. כצעד ראשון בשיפור ביטחון הסייבר התבצע שינוי ארגוני במערך הסייבר הבריטי והוחלט על הקמת "מרכז ביטחון הסייבר הלאומי" (National Cyber Security Centre – NCSC),[16] שקיבל את אחריות הביצוע האופרטיבי המדינתי על כל תחום ההגנה של ביטחון הסייבר בבריטניה. אחריות זו כוללת, בין השאר, שיתוף ידע, התמודדות עם נקודות תורפה והובלה מקצועית של נושא הסייבר ברמה הלאומית. מכיוון שלמערכת הביטחון הבריטית יש יכולת חזקה להגן על מערכותיה הפנימיות והיא נדרשת לפעילות אופרטיבית גמישה ועצמאית, הוחלט כי "מרכז ביטחון הסייבר הלאומי" ישתף פעולה עם "מרכז מִבצעֵי ביטחון הסייבר" (Cyber Security Operations Centre) של הצבא הבריטי, תוך יצירת פלטפורמה בין־ארגונית שתאפשר לצבא לקחת חלק בהגנה מול אירועי סייבר בעלי פוטנציאל לפגיעה אסטרטגית ברמה הלאומית.

"מרכז ביטחון הסייבר הלאומי" הושק רשמית באוקטובר 2016 כחלק ממטה ה־GCHQ. החזון שמאחורי הקמתו היה ליצור גוף מטה שיתכלל את ניהול אירועי תקיפות סייבר בחירום, יספק הנחיה בשגרה ובחירום וישמש כמוקד ידע לקהילת הסייבר הבריטית, וכן יהווה גוף מקשר בין הממשלה לתעשייה. המרכז איגם בתוכו גופי ביטחון סייבר קיימים, ובהם "המרכז להערכת סיכוני סייבר" (Centre for Cyber Assessment), ה־CERT הלאומי, וכן את הזרוע של GCHQ שעסקה באבטחת מידע (CESG). בנוסף לכך, המרכז החדש קיבל את האחריות על כל נושאי הסייבר שהיו לפני כן תחת אחריותו של "המרכז לאבטחת תשתיות לאומיות" (Centre for the Protection of National Infrastructure).

15 "The Cyber Threats to UK Businesses, 2016/2017 Report", *NCSC & NCA*, March 14, 2017 http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file.

16 "The Launch of the National Cyber Security Centre", *National Cyber Security Centre*, February 13, 2017, https://www.ncsc.gov.uk/news/launch-national-cyber-security-centre.

תפיסת ההגנה

תפיסת ההגנה הבריטית בתחום הסייבר מבוססת על הצורך לגבש מענה מדינתי לחיזוק ההגנה ברמה הלאומית, לצד הנחיית התעשייה לגיבוש צעדים לאבטחת תשתיות קריטיות לאומיות במגזרים חיוניים, כמו אנרגיה ותחבורה. תפיסת ההגנה הבריטית אמורה להתממש באמצעות שיתוף פעולה עם התעשייה,[17] כולל מיקור חוץ, במטרה להשתמש בטכניקות הגנה אוטונומיות להפחתת השפעתן של תקיפות סייבר המבוצעות על ידי האקרים, ועצירת וירוסים ודואר זבל לפני שהם מגיעים לקורבנות התקיפה. אחד המדדים להצלחה שהוגדרו על ידי הממשלה בהקשר זה הינו משך הזמן שבו אתר זדוני המפיץ נוזקות נשאר פעיל. הסטטיסטיקה בבריטניה הצביעה בעבר על משך זמן של כחודש, לעומת כיומיים בלבד כיום. מדד נוסף הוא מספר אתרי מתקפות דיוג הרשומים בבריטניה אשר מוּרדים מהרשת לאחר כשעה (בעבר משך הזמן להורדתם היה כ־24 שעות).

תפיסת ההגנה הבריטית קובעת עוד כי חלק גדול מהשקעות הממשלה בביטחון סייבר יוקצה לחיזוק יכולות הסייבר של סוכנויות אכיפת החוק וליצירת מענה הגנתי שיגדיל משמעותית את מחיר פשעי הסייבר, וכן לגיבוש שותפויות בין־לאומיות ולבניית יכולות סייבר התקפיות כתגובה לתקיפות מדינתיות נגד בריטניה. כחלק מההתעצמות בתחומים אלה, גויסו יותר מחמישים חוקרי סייבר ומומחים טכנולוגיים ליחידה הלאומית להתמודדות עם פשיעת סייבר ותוקצבו עשרות מיליוני ליש"ט ללחימה בפשעי סייבר.

הגנת סייבר אקטיבית

כדי ליישם את צעדי הביטחון הנדרשים ברמה הלאומית, גובשה תפיסה הנקראת "הגנת סייבר אקטיבית" (Active Cyber Defence – ACD).[18] בהקשר המסחרי, המושג ACD מתייחס בדרך כלל לניתוח סיכוני ביטחון סייבר, לפיתוח הבנה של איומים ברשת וליישום צעדים פרו־אקטיביים הנדרשים כמענה הגנתי לכך. באסטרטגיית הסייבר הלאומית הבריטית, הממשלה בחרה ליישם את התפיסה המסחרית בהקשר רחב יותר: להביא לידי ביטוי את יכולותיה הייחודיות כדי להשפיע על הצעדים שיינקטו נגד מגוון האיומים בסייבר. לפי תפיסה זאת, "הרשת" מייצגת את כל מרחב הסייבר הבריטי ברמת המקרו. כדי לעמוד ביעד ולצמצם את איומי הסייבר נגד בריטניה, כולל מצד קבוצות פשע מאורגנות וישויות מדינתיות

17 דוגמה לשיתוף פעולה עם התעשייה היא עידוד של ה־CERT הלאומי ליצירתם של אשכולות (Clusters) לשיתוף והעמקת ידע בנושאי הגנת סייבר, הפזורים ברחבי בריטניה ופועלים בצורה התנדבותית, עצמאית ולא פורמלית. ראו רשימת האשכולות: https://www.ukcybersecurityforum.com/cyber-security-clusters.

18 "National Cyber Security Strategy 2016-2021", p. 33.

בעלות כוונות זדון, יורחבו סמכויותיהם ויכולותיהם של GCHQ, משרד ההגנה ו"סוכנות הפשיעה הלאומית".

הצלחתה של תפיסת "הגנת הסייבר האקטיבית" תימדד על פי התוצאות הבאות:[19]

- הקמת מערך הגנה רחב שיקשה על ניסיונות לתקיפות דיוג, SMS וזיופים (Spoofing) כחלק מקמפיינים של הנדסה חברתית.
- חסימת נוזקות זדוניות.
- הבטחת התנועה באינטרנט ותקשורת נגד ניסיונות Rerouting.
- הגברת יכולות ה־GCHQ, "סוכנות הפשיעה הלאומית" והצבא הבריטי לתת מענה הגנתי יעיל מפני תקיפות סייבר אסטרטגיות.

שיתוף ידע

אחת התובנות המרכזיות של אסטרטגיית הסייבר הבריטית היא שרוב התקיפות נעשות בכלי תקיפה בסיסיים שהיערכות נכונה של ארגונים יכולה למנוע אותן. לשם כך יצר GCHQ פלטפורמה לשיתוף ידע וכתב מדריך למשתמש בשם *Cyber Essentials*, שהינו שימושי בעיקר להגנה על עסקים קטנים ובינוניים.[20] "מרכז ביטחון הסייבר הלאומי", מצידו, כתב מדריך למשתמש בנושאי הערכת סיכוני סייבר, בשם "עשרה צעדים לביטחון סייבר".[21] למהלכים אלה יש גם משמעויות רגולטוריות הנוגעות לגיבוש הַתֶּקן על פיו נדרשים ארגונים בבריטניה להיערך מבחינת איומי סייבר.[22]

גורם נוסף בתחום ביטחון הסייבר בבריטניה הוא "המשרד לביטחון סייבר ואבטחת מידע" (Office of Cyber Security and Information Assurance – OCSIA). מדובר בגוף הפועל ברמה הממשלתית ותפקידו לתמוך במשרדי הקבינט וב"מועצה לביטחון לאומי" במכלול היבטי הסייבר, להעניק הכוונה אסטרטגית ולתאם את תוכניות ביטחון הסייבר ברמה הממשלתית.[23] "המשרד לביטחון סייבר ואבטחת מידע" עובד בשיתוף פעולה עם משרדי ממשלה וסוכנויות ממשלתיות, כגון משרד ביטחון הפנים, משרד ההגנה, משרד החוץ, משרד התקשורת ו־GCHQ.

---

19 שם, עמ' 35.

20 "Cyber Essentials", *HM Government*, http://www.cyberaware.gov.uk/cyberessentials/

21 "10 Steps to Cyber Security", *NCSC*, April 10, 2016, https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

22 "Minister for Digital and Culture Matt Hancock's speech at the Cyber Security Institute of Directors Conference in London", March 27, 2017, https://www.gov.uk/government/speeches/matt-hancocks-cyber-security-speech-at-the-institute-of-directors-conference.

23 ראו אתר OCSIA: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.

"המשרד לביטחון סייבר ואבטחת מידע" גם אמון על הקצאת משאבים ותכלול בין משרדי הממשלה בתחום הסייבר, וכן עוסק בהיבטים של מדיניות סייבר בממשק מול המגזר הפרטי. בהמשך מתוכנן לקום גוף בשם Emerging Technology and Innovation Analysis Cell (ETIAC). גוף זה אמור לזהות התפתחויות, איומים והזדמנויות טכנולוגיות לטובת הביטחון הלאומי וגופי הסייבר הממשלתיים.[24]

גוף נוסף בעל אחריות מדינתית בנושאים הקשורים לפשעי סייבר הינו "יחידת פשעי הסייבר הלאומית" (The National Cyber Crime Unit – NCCU).[25] היחידה, הכפופה ל"סוכנות הפשיעה הלאומית", החלה בפעילות אופרטיבית בשנת 2013. היא מובילה את תחום התגובה המדינתית לפשעי סייבר, כולל תמיכה בשותפיה במערכת הביטחונית, וכן את תיאום התגובה המדינתית לרוב פשעי הסייבר החמורים במדינה. היחידה פועלת בשיתוף פעולה עם יחידות פשעי סייבר מחוזיות (Regional Organized Crime Units – ROCUs), יחידת פשעי הסייבר של משטרת המטרופולין (של לונדון) (Metropolitan Police Cyber Crime Unit – MPCCU), גורמי תעשייה, גופי ממשל ויחידות אכיפת חוק בין־לאומיות.

בבריטניה פועלת החל משנת 2013 פלטפורמת שיתוף הידע Cyber-Security Information Sharing Partnership. פלטפורמה זו כוללת יותר מאלפיים ארגונים ציבוריים וחברות פרטיות. לחברות ולארגונים הבריטיים ישנה גם נגישות ליוזמת X-Force Initiative של חברת IBM, המסַפקת יותר מ־700 טרה בייט של מידע על איומי סייבר.[26]

מחקר ופיתוח

עידוד המו"פ בא לידי ביטוי בהחלטה להקים מרכזי חדשנות סייבר שיגבשו פתרונות סייבר מתקדמים ויהוו תשתית להקמת חברות סייבר חדשות, וכן בהשקת קרן למימון חדשנות בסייבר, בתמיכה בחברות הזנק ובמחקרים אקדמיים בשיתוף התעשייה. בסך הכול הוקצו במסגרת אסטרטגיית הסייבר של 2016 כ־165 מיליון ליש"ט לתמיכה בחדשנות בנושאי הגנה וביטחון סייבר.[27]

בנוסף לאלה מקימה בריטניה "מוסד למחקר ביטחון סייבר" (Cyber Security Research Institute), שיאגד את האוניברסיטאות המובילות במדינה לפעילות לחיזוק אבטחת מכשירים חכמים. "מרכז ביטחון הסייבר הלאומי" ו־GCHQ, מצידם, תומכים בחדשנות ובמחקר בנושאי סייבר לגילאי בית ספר. אחת התוכניות אותה

24 יש לציין כי כיום פועל צוות ייעוץ לחשיבה אסטרטגית בקבינט בשם Secretary's Advisory Group on Horizon Scanning (CSAG).

25 ראו פרטי הסוכנות: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

26 "Progress and Research in Cybersecurity", p. 42.

27 שם, עמ' 10.

מממן GCHQ היא תוכנית Cyber First, במסגרתה לוקחים חלק כ־2500 תלמידי בית ספר בגילאי 11–17 בקורסי סייבר חינמיים.[28] בין השאר כוללת התוכנית תחרות סייבר לבנות בגילאי 13–15.[29]

כ־250 סטודנטים הלומדים מקצועות רלוונטיים במסגרות אקדמיות מקבלים בכל שנה מלגות בשווי 4,000 ליש"ט לשנה, כאשר הכוונה היא להגיע למספר של אלף סטודנטים בשנת 2020. "מרכז ביטחון הסייבר הלאומי" ו־GCHQ משתפים פעולה עם כעשרים אוניברסיטאות מובילות ברחבי בריטניה בהעברת עשרים קורסים לתלמידי תואר שני, בהם ממשיכים הסטודנטים לשנה נוספת של לימודים אינטגרטיביים מתקדמים בפורנזיקה דיגיטלית, מדעי המחשב וסייבר. "מרכז ביטחון הסייבר הלאומי" גם יצא במספר יוזמות מחקריות הכוללות, בין השאר, תוכנית להקמת 13 מרכזים אקדמיים למחקר מצוינות בסייבר ומתן מלגות לשלושים תלמידי תואר שלישי שנבחרים מתוך מרכזי המצוינות. "מרכז ביטחון הסייבר הלאומי" גם הקים את "מרכז חדשנות הסייבר הממשלתי" (Cyber Security Innovation Centre) המשמש כחממה לחברות הזנק.

GCHQ פרסם ב־2017 קול קורא למימון מיזמים ומחקרים והקים תוכנית האצה לחברות הזנק בתחום הסייבר.[30] תוכנית האצה זו כוללת בשלב הראשון שבע חברות הזנק הזוכות לתמיכה מתאגידים כגון "טלפוניקה" ו"סיסקו". הכוונה של GCHQ היא למצוא חברות הזנק, דוגמת Cyber Owl, שפיתחה מערכת התרעה מוקדמת המספקת מודיעין בזמן אמת; Status Today, שפיתחה פלטפורמת בינה מלאכותית כדי להבין התנהגות אנושית במקום העבודה ולמנוע מתקפות מתוך הארגון; ו־Elemendar, שהיא פלטפורמת בינה מלאכותית לניתוח דוחות סיכונים.

יוזמה המתמקדת בשיתוף פעולה ממשלתי עם התעשייה במימון מחקרי סייבר באקדמיה היא תוכנית Cyber Invest. ממשלת בריטניה הכריזה על התוכנית בשנת 2015, כחלק משיתוף פעולה בינה ובין התעשייה המקומית במטרה ליישם מחקרי סייבר במישור המסחרי. תוכנית זאת היא חלק מ־165 מיליון ליש"ט שהוקדשו להגנה וחדשנות בסייבר במטרה לסייע לחברות הזנק להגיע להישגים מסחריים,

28 "Applications open for GCHQ's Cyber Summer Schools", *GCHQ,* May 20, 2016, https://www.gchq.gov.uk/press-release/applications-open-gchqs-cyber-summer-schools.

29 "National Challenge will Develop Schoolgirls' Cyber Security Skills", *GCHQ*, January 18, 2017, https://www.gchq.gov.uk/press-release/national-challenge-will-develop-schoolgirls-cyber-security-skills.

30 "The first-ever GCHQ-backed accelerator programme for cyber security start-ups concludes today, with all parties involved hailing it as a huge success", *Wayra*, March 30, 2017, https://wayra.co.uk/first-cyber-security-start-ups-graduate-from-unique-gchq-cyber-accelerator-programme/

וכן לסייע ליוזמות לא מסחריות בתחום הסייבר.[31] בשנה שלאחר ההכרזה על התוכנית התחייבו 18 חברות להשקיע 6.5 מיליון ליש"ט במהלך חמש השנים הבאות בתחום זה.

גוף מחקרי נוסף בתחום ביטחון הסייבר הוקם בשנת 2013 – "מכון המחקר למדעי ביטחון הסייבר" (The Research Institute in Science of Cyber Security).[32] ייעודו הוא פיתוח מדעי ויצירת סטנדרטים ושיטות פעולה לטובת מקבלי ההחלטות בתחום הסייבר. המכון ממומן על ידי ה־GCHQ ו"המועצה למחקר בהנדסה ופיזיקה" (The Engineering and Physical Sciences Research Council).

פעילות בין־לאומית

בריטניה מימנה בשנת 2016 תוכניות לחיזוק החוסן הלאומי בתחום הסייבר ולתמיכה ב־35 פרויקטים בכשבעים מדינות בעולם, בעלות של 3.5 מיליון ליש"ט. אחת המדינות איתן מקיימת בריטניה תוכניות מחקר משותפות בתחום הסייבר היא סינגפור. תוכנית מו"פ משותפת לשתי המדינות בנושאי ביטחון סייבר הושקה ב־2015, והיא כוללת מימון למחקרים בתחום זה.[33] מאז השקת התוכנית נערכו במסגרתה שש תוכניות מחקר משותפות בעלות מוערכת של 2.4 מיליון ליש"ט.[34]

בריטניה חתומה על הסכמי שיתוף פעולה בתחום הסייבר עם מדינות רבות ברחבי העולם ומקיימת שיתופי פעולה אסטרטגיים בתחום זה עם ארצות הברית, אוסטרליה, ניו זילנד וקנדה.[35] שיתוף הפעולה הבין־לאומי של בריטניה בתחום פשיעת הסייבר נמצא באחריות "סוכנות הפשיעה הלאומית", המקיימת קשרים עם "אינטרפול", "יורופול" וסוכנויות נוספות.[36] ממשלות בריטניה גם מקדמות בשנים האחרונות דיאלוגים אסטרטגיים עם מדינות שונות בתחום הסייבר. כך, ב־2016 גיבשה בריטניה מסמך הבנות עם סין להעמקת קשרי שתי המדינות בתחום הסייבר, כולל בניית מכניזם לשיתוף מידע מודיעיני, שיתוף פעולה במצבי חירום

31 "Progress and Research in Cybersecurity", p. 60.

32 ראו אתר התוכנית: http://www.riscs.org.uk.

33 ראו אתר התוכנית: https://www.nrf.gov.sg/funding-grants/international-grant-calls/joint-singapore-uk-research-in-cyber-security.

34 Ankit Panda, Conrad Prince, "On the United Kingdom's Cyber Strategy and Asia", *The Diplomat*, October 15, 2016, http://thediplomat.com/2016/10/conrad-prince-on-the-united-kingdoms-cyber-strategy-and-asia/.

35 "What is the Five Eyes Intelligence Alliance?", *France 24*, March 17, 2017, http://www.france24.com/en/20170317-what-five-eyes-intelligence-alliance.

36 "International Cooperation", *The National Crime Agency*, http://www.nationalcrimeagency.gov.uk/about-us/working-in-partnership/international-cooperation.

ועוד.[37] באותה שנה גם יצאו ממשלות בריטניה והודו בהצהרה משותפת על שיתוף פעולה אסטרטגי ביניהן, כולל בתחום הסייבר.[38]

פערים ביישום האסטרטגיה הבריטית

למרות הגדלה משמעותית של התקציב הבריטי להגנת מרחב הסייבר לשנים 2016–2021, וכן הארגון מחדש ואיגום הסמכויות של זרועות הגנת הסייבר בבריטניה, אתגרים ופערים רבים מַקשים עדיין על הטמעתה ויישומה האפקטיבי של אסטרטגיית הסייבר הבריטית: ראשית, המדיניות של השפעה פעילה על תהליכי פיתוחה של חדשנות טכנולוגית לטובת הגנת הסייבר, אותה נקטה ממשלת בריטניה, דורשת יצירת איזונים בין המרכיבים הביטחוניים, הטכנולוגיים, הכלכליים והחברתיים. למרות זאת, נראה כי המרכיב הביטחוני הוא דומיננטי ביחס למרכיבים האחרים ומשמש ציר מרכזי שדרכו פועלת הממשלה ליצור תנאים שיאפשרו התפתחות ידע וסביבה טכנולוגית חדשנית. מהזווית ההגנתית־ביטחונית, ובמיוחד לאור המבנה ההיסטורי של מערכת הביטחון והאכיפה הבריטית, טבעי הוא שריכוז יכולת הגנתית ברמה גבוהה ייעשה באמצעות זרועות ה־GCHQ; אך ציר זה מהווה חיסרון בכול הנוגע לממשקים המתקיימים מחוץ למערכת הביטחון הבריטית, שיכולים לסייע בהפריה הדדית בין המערכת הביטחונית ובין המערכת האזרחית, כגון פיתוח ידע אקדמי, הכשרת אנשי מקצוע איכותיים, קשרי גומלין בין התעשייה לאקדמיה, פיתוח עסקי וחדשנות טכנולוגית. הדומיננטיות של GCHQ גם מקשה על בריטניה בכול הקשור לשיתוף פעולה עם חברות טכנולוגיה גלובליות. כלומר, בחירתם של מעצבי התפיסה האסטרטגית הבריטית להתבסס על המשאבים הקיימים בבריטניה להגנה מפני איומי סייבר יוצרת כשל מובנה המציב אתגרים בפני יישום המענה הרצוי. כשל זה בא לידי ביטוי, בין השאר, בהיעדר עידוד משמעותי לחברות טכנולוגיה גלובליות לקדם פיתוח, מחקר ועשייה עסקית משמעותית בבריטניה.

שנית, יש המצביעים על דמיון בין המבנה והמדיניות של מערך הסייבר הבריטי לאלה של מדינת ישראל. השוואה זו לא עומדת במבחן התוצאה בכול הקשור לקשיים של המודל הבריטי לאפשר מערכת סביבתית יעילה של ביטחון, תעשייה, חינוך ואקדמיה. כך, למשל, ישראל שומרת על רמת תחרותיות גבוהה בשוק הסייבר העולמי, בין השאר כתוצאה מכך שבוגרי יחידות טכנולוגיות במערכת

37 "China-UK High Level Security Dialogue: Communique, Policy Paper", *Cabinet Office*, June 13, 2016, https://www.gov.uk/government/publications/china-uk-high-level-security-dialogue-official-statement/china-uk-high-level-security-dialogue-communique.

38 "Joint Statement between the Governments of the UK and India, Press Release", *Prime Minister Office*, November 7, 2016, https://www.gov.uk/government/news/joint-statement-between-the-governments-of-the-uk-and-india.

הביטחון שלה הקימו חברות מצליחות המספקות מוצרים ביטחוניים דואליים המיועדים לשימוש ביטחוני ואזרחי כאחד, ו/או טכנולוגיות ביטחוניות שניתן למצוא להן יישומים אזרחיים. יתרונה היחסי של מערכת הביטחון הישראלית הוא בכך שהיא לא בהכרח ממציאה את הטכנולוגיה, אלא מבצעת התאמות של פיתוחים אזרחיים הקיימים בשוק הפרטי בהתאם לצרכיה. לעומת זאת, המצב בבריטניה נראה שונה, ובמקרים רבים אף הפוך: המערכת הביטחונית הבריטית תורמת את חלקה לפיתוח טכנולוגי, שרק חלקו עובר לאחר מכן לשוק האזרחי. כתוצאה מכך, המנגנון הממשלתי הבריטי מצמצם את יכולת תעשיית הסייבר המקומית לשמור על יתרון יחסי במציאות של תחרות גלובלית וגם מול איומים מתהווים. מצב זה יישמר כל עוד ממשלת בריטניה תמשיך להשקיע את מרבית תקציב הגנת הסייבר בסוכנויות האמונות על כך. יש להניח כי בתקציב הממשלתי להגנת סייבר המיועד לסוכנויות הביטחון והמודיעין הבריטיות, כגון GCHQ, משאבים רבים מופנים גם כיום להתקפה ולא להגנה, ויותר משאבים מופנים להגנת תשתיות קריטיות ולא להגנת תשתיות אחרות. כמענה לפער זה, על בריטניה לשקול את ניתוקו המלא או החלקי של "מרכז ביטחון הסייבר הלאומי" מ־GCHQ ולהפוך אותו לגוף בעל מאפיינים אזרחיים יותר שיַקלו על הנגשתו למגזר הפרטי. בריטניה גם נדרשת למצות באופן נכון יותר מידע ופתרונות טכנולוגיים המועברים מהמגזר הביטחוני הבריטי לתעשייה האזרחית וחוזר חלילה. דרך נכונה ליישם זאת היא, בין השאר, גישה הוליסטית שתחלק את המשאבים בצורה מאוזנת יותר בין ביטחון ובין השקעות בחינוך, באקדמיה ובמגזר הפרטי.

שלישית, יציאת בריטניה מהאיחוד האירופי צפויה להיות בעלת השלכות על ביטחון הסייבר הלאומי שלה. העזיבה תביא, ככול הנראה, ליציאה של בריטניה מארגונים באיחוד האירופי בהם היא חברה כיום, כגון "מרכז פשיעת הסייבר האירופי" (European Cybercrime Centre), ובכך היא לא תהיה עוד שותפה למאמצי מניעת פשיעת סייבר באיחוד. טרם ברור מה תהיה המדיניות הבריטית לגבי נושאים רגולטוריים משותפים למדינות האיחוד האירופי, כגון "רגולציית אבטחת המידע" (General Data Protection Regulation – GDPR), ועד כמה היא תשתנה בעקבות עזיבת בריטניה את האיחוד.[39] אתגר שאיתו תיאלץ בריטניה להתמודד ביתר שאת בעקבות עזיבת האיחוד האירופי הינו גיוס כוח אדם איכותי למקצועות הסייבר. ביטחון סייבר התווסף בנובמבר 2015 לרשימת המקצועות בהם ישנו מחסור בבריטניה, דבר שאִפשר לאזרחים מחוץ לאיחוד האירופי להגיש בקשה לאשרת עבודה שם. עזיבת בריטניה את האיחוד עלולה להביא למצב הפוך,

39 החלטה במסגרת GDPR, שצפויה להיכנס לתוקף באיחוד האירופי במהלך 2018, היא דרישה מחברות הרשומות באיחוד להודיע לממשלותיהן על תקיפות סייבר נגדן בתוך 72 שעות. ראו גם אתר אבטחת המידע האירופי: http://www.eugdpr.org /

בו בעלי מקצוע בריטיים בתחום הסייבר יבחרו לעבוד במדינות אחרות (בהן רמת ההכנסה ואפשרות המוביליות יהיו גבוהות יותר לאחר ה"ברקזיט"). כמו כן, בריטניה תיאלץ למצוא דרכים תקציביות לממן מחקר אקדמי בתחומים טכנולוגיים, שכיום ממומן חלקית מתקציבי האיחוד האירופי. מענה לכך בטווח הקצר הינו הסטת משאבים שיועדו למחקר ופיתוח ולמימון קרנות של האיחוד האירופי לטובת פתיחת קרנות ייעודיות למחקרים אקדמיים במרכזי הידע הבריטיים. לעומת זאת, עזיבת האיחוד האירופי לא צפויה לפגוע בשותפויות הסייבר האסטרטגיות של בריטניה עם מדינות ה־"Five Eyes" (אוסטרליה, קנדה, ניו זילנד, בריטניה וארצות הברית).[40]

סיכום

בריטניה קיבלה החלטה אסטרטגית ארוכת טווח בנושא ביטחון הסייבר הלאומי, שכוללת חיזוק החוסן הלאומי במרחב הסייבר בכלל ובמרחב הדיגיטלי בפרט. זאת, באמצעות השקעות ממשלתיות המכוונות ליצירת הון אנושי, החל מרמת בתי הספר, כולל הקמת מרכזי מצוינות למחקרי סייבר ותוכניות האצה בסייבר לחברות הזנק. חלק מהמשאבים מוקדשים לארגון מחדש של מערך הסייבר ההגנתי ולגיוס מומחי סייבר לרשויות אכיפת החוק וסוכנויות הביון של בריטניה. גולת הכותרת של האסטרטגיה הבריטית היא הקמת "מרכז ביטחון הסייבר הלאומי", האמון על בניית גשר בין הממשלה והתעשייה ועל הנחייה וניהול של מצבי חירום, כולל נגד תקיפות סייבר המכוונות לתשתיות לאומיות קריטיות.

לצד בניית יכולות הרתעה התקפיות, פועלת בריטניה בטווח הקצר לצמצום תקיפות סייבר "בסיסיות", המהוות את רוב המתקפות עליה. לצד זאת, בריטניה גיבשה חזון, לפיו נושאים כמו מערכות אוטונומיות, "האינטרנט של הדברים" וטלפונים חכמים, שיהוו את מרבית האיומים בטווח הבינוני, זוכים כבר היום למענה. זאת, על ידי הקמת תשתית מחקרית אקדמית ומסחרית שתנסה להתמודד עם האתגרים והאיומים לאורך זמן.

אסטרטגיית ביטחון הסייבר הלאומית של בריטניה לשנים 2016–2021, המתוקצבת בכ־1.9 מיליארד ליש"ט, הציבה במוקד את יישום התפיסה של הסתמכות עצמית על המשאבים הטכנולוגיים והאנושיים לצורך הגנה, וכן את יצירתם של מנגנוני הרתעה ושיתופי פעולה בין־לאומיים. נראה כי בניגוד לעבר, בו GCHQ וארגוני הביטחון הבריטיים הסתמכו על מערכותיהם שלהם בכול מה שנוגע לתחומי המו"פ הביטחוניים, התפיסה הבריטית הנוכחית מעודדת ביזור יכולות ומחקר, ואף כוללת אסטרטגיה חדשה, בה GCHQ פתוח יותר מבעבר לשיתופי

40 "The Implications of Brexit on UK Cyber Policy", *Council on Foreign Affairs*, June 28, 2016, https://www.cfr.org/blog/implications-brexit-uk-cyber-policy.

פעולה עם גופים אזרחיים וציבוריים כדי לקדם חדשנות טכנולוגית, פיתוח הון אנושי וצמיחת שוק הסייבר הבריטי האזרחי.

למרות כל המאמצים שנעשו עד כה, אתגרים ופערים רבים ממשיכים להקשות על הטמעת אסטרטגיית הסייבר הבריטית. בין שאר האתגרים – ריכוזיות היתר של מבנה הגנת הסייבר הבריטי בראשות GCHQ ועזיבתה הצפויה של בריטניה את האיחוד האירופי. מענה אפשרי לאתגרים אלה הינו חלוקת משאבים מאוזנת יותר בין השקעה בביטחון סייבר ובין השקעות בחינוך, באקדמיה ובמגזר הפרטי.