דו"ח מדיניות וביטחון סייבר

מרץ 2023

דורון פלדמן, אופיר בראל,

דניאל כהן, ניצן הררי

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

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Website: sectech.tau.ac.il | Tel: +972 (3) 6406041 | Email: icrc@tauex.tau.ac.il

תוכן עניינים

תקציר חודשי

משרד ראש המודיעין הלאומי האמריקני (ODNI) הזהיר בדו"ח האיומים השנתי שלו כי במקרה של עימות צבאי עם סין, היא צפויה לבצע מתקפות סייבר על נכסים צבאיים ותשתיות חיוניות בארה"ב. על רקע זה, גורמי ממשל בכירים ציינו כי מחלקות האוצר והמסחר מנסחות תכנית שתאסור על השקעות אמריקניות בתחומי הטכנולוגיות המתקדמות בסין, מחשש כי יריביה ינצלו אותן לצורך פגיעה בביטחונה הלאומי. בנוסף, חתם הנשיא ביידן על צו נשיאותי האוסר על ממשלת ארה"ב להשתמש ברוגלות מסחריות; מחלקת ההגנה פרסמה אסטרטגיה חדשה לשנים 2023-2027 ומטרתה לצמצם את הפער בכוח האדם המיומן במקצועות הסייבר ברחבי המחלקה, באמצעות שיפור הליכי הגיוס, הניהול וההכשרה של העובדים.

מספר מדינות מערביות, בהן בריטניה, צרפת, הולנד וניו זילנד אסרו על השימוש באפליקציית הרשת החברתית הסינית, TikTok על גבי מכשירים ממשלתיים, מחשש לפגיעה בביטחון הלאומי; כלי תקשורת אמריקני פרסם תחקיר המבוסס על מסמכים מודלפים ולפיו גופי ביון וביטחון מרוסיה רכשו טכנולוגיות מחברת התוכנה הרוסית, TNC Vulkan כדי לבצע התקפות סייבר, להפיץ מידע כוזב ברשתות החברתיות ולנטר את תעבורת הרשת במדינה; בכוונת אוקראינה לנסח חוק שיסדיר את מעמדה של קבוצת ההאקטיביסטים המתנדבים, צבא ה-IT, וישלב אותה ככוח עתודה פעיל כחלק מהצבא הסדיר במדינה; וועדה בפרלמנט האירופי אישרה מסמך המחייב את מוסדות האיחוד לדווח על אירועי סייבר בתוך 24 שעות מרגע גילויים וכן לדווח על השלכותיהם לא יאוחר מ-72 שעות.

בהמשך לפרסום אסטרטגיית אבטחת הסייבר הלאומית של ארה"ב, קידמו הממשל והקונגרס הטמעה של דרישות אבטחת סייבר בסיסיות, שיחייבו את מדינות ארה"ב להעריך את מידת האבטחה בקרב מערכות המים שברשותן וכן ידרשו מבעלי ומפעילי תשתיות חשמל, לנהל סיכוני אבטחת סייבר בשרשראות אספקה של מערכות חשמל מבוזרות. כמו כן, הציג הממשל לתגובות הציבור הנחיות שיחייבו גופים מענף מסחר המניות לדווח לו באופן מיידי על תקריות סייבר; תאגיד MITRE הציג אב-טיפוס לאפליקציית רשת, המיועדת לסייע לצוותי אבטחת סייבר להגדיר ולספק מענה לסיכוני אבטחה בשרשרת האספקה, שמקורם בספקי שירותים, תוכנה וקושחה.

רשות הימאות והנמלים של סינגפור הודיעה על כוונתה להקים עד לשנת 2025 מרכז אבטחת סייבר ותפעול ימי, שמטרתו לנטר אחר איומי סייבר ולהתריע מפניהם בזמן אמת, להקל על שיתוף המידע בתחום אבטחת הסייבר בין גופים ממגזר הימאות, לספק הכשרה ופלטפורמה לתרגילים עבור מומחי אבטחה ועוד; ממשלת בריטניה פרסמה אסטרטגיה לאומית חדשה לשנים 2024-2034 ותקציב בסך 2.5 מיליארד ליש"ט (כשלושה מיליארד דולר) המיועדים להפוך אותה למדינה מובילה בתחום המחשוב הקוונטי.

ממשל, אסטרטגיה ומדיניות

החודש פרסם **הבית הלבן** את מסמך אסטרטגיית אבטחת הסייבר הלאומית, הקוראת לממשל הפדראלי לקדם שיתופי פעולה עם ממשלות ברמת המדינה (state level), המגזר הפרטי והתעשייה, החברה האזרחית ובעלות בריתה של ארה"ב, במטרה לשפר את מידת הגנת הסייבר של תשתיות חיוניות; לסכל תקיפות סייבר ומתקפות כופרה מצד גורמים זדוניים; להעביר חלק מאחריות האבטחה מיחידים ועסקים קטנים אל ארגונים גדולים. לצורך כך, יגבש הממשל חקיקה שתגדיר כלפי חברות המייצרות ומשווקות מוצרי ושירותי תוכנה, דרישות אבטחה מחייבות; לעודד השקעות בטכנולוגיות חדשניות ובכוח אדם המיומן במקצועות הסייבר; ולקדם שיתופי פעולה בין-לאומיים עם בעלות בריתה של ארה"ב במאבק באיומי סייבר.[1] ב-29 במרץ העריך דובר **משרד ראש הסייבר הלאומי** (ONCD) כי עד לסוף חודש יוני 2023, יפרסם הבית הלבן תכנית ליישום האסטרטגיה.[2]

האסטרטגיה החדשה עשויה להוביל לשינוי מהמדיניות הקוראת לעמידה וולונטרית בדרישות האבטחה, שהיוותה נר לרגלם של מקבלי ההחלטות בארה"ב בשנים האחרונות, לעבר הטמעת רגולציה מקיפה יותר שתחייב ארגונים וחברות אמריקניות, במיוחד מענפי התשתיות החיוניות, לעמוד בדרישות אבטחת סייבר מינימליות. האסטרטגיה ייחודית היות והממשל האמריקני מבקש לרתום באופן רשמי את המגזר הפרטי והתעשייה המקומית להגנת הסייבר הלאומית. על רקע זה, נראה כי **אוסטרליה** הולכת בדרכה של ארה"ב להעברת אחריות רבה יותר למגזר הפרטי בזיהוי ומתן מענה לחולשות אבטחת סייבר. ב-22 במרץ, הצהירה שרת הפנים והשרה לאבטחת סייבר בממשלה, קלייר אוניל (Clare O'Neil), כי הממשלה וצוות המומחים לפיתוח אסטרטגיית הסייבר הלאומית החדשה[3] שוקלים לקדם צעדים חדשים, שיסיטו את האחריות לאבטחת מוצרים מספקים ונותני שירותים אל המגזר הפרטי, בייחוד חברות תקשורת, אבטחת סייבר ושירותי תוכנה.[4]

בד בבד עם פרסום האסטרטגיה, החודש המשיך הממשל לקדם יוזמות שמטרתן לשמר את יתרונה של ארה"ב בחלק מתחומי הטכנולוגיה, אל מול יריבותיה.

[1] קישור למסמך האסטרטגיה: https://bit.ly/41Oeo2j. להרחבה ופרשנות: https://bit.ly/3mSIbHq ; http://bit.ly/3FBpHBw
[2] http://bit.ly/3K1sqWl
[3] הצוות מונה בדצמבר 2022, וכולל את מפקד חיל האוויר המלכותי של אוסטרליה לשעבר, מל האפלד (Mel Hupfeld), מנכ"ל חברת התקשורת Telstra לשעבר, אנדרו פן (Andrew Penn) ומנכ"לית מרכז המחקר השיתופי באבטחת סייבר, רייצ'ל פאלק (Rachael Falk).
[4] https://bit.ly/3zpzQ0T

ב-3 במרץ, דיווח ה-Wall Street Journal כי **מחלקות האוצר והמסחר** מנסחות תכנית חדשה שתאסור השקעות אמריקניות בתחומי הטכנולוגיות המתקדמות מחוץ לשטחי ארה"ב, בהן מחשוב קוונטי ובינה מלאכותית מחשש לפגיעה בביטחונה הלאומי. מטרת התכנית שתפורסם בזמן הקרוב, למנוע מיריביה של ארה"ב לנצל את ההון והמומחיות האמריקניים בתחומים הטכנולוגיים כדי לשמר את יתרונה, אך מבלי להטיל נטל רגולטורי על משקיעים ועסקים בארה"ב. אף כי התכנית לא כוללת התייחסות למדינה ספציפית, מתוך עקרונותיה המתגבשים עולה כי היא מיועדת להגביל בעיקר השקעות אמריקניות בסין.[5]

בה בעת, ב-27 במרץ, חתם **הנשיא ביידן** על צו נשיאותי האוסר על ממשלת ארה"ב להשתמש ברוגלות מסחריות, מחשש לפגיעה בביטחונה הלאומי של ארה"ב ועקב חשש מהשפעה או שליטה ישירה פוטנציאלית של ממשלות זרות על חברות אלו. עם זאת, הצו מתיר לסוכנויות פדראליות להשתמש ברוגלה, בתנאי שהן מצדיקות את השימוש ומיידעות על כך את עוזר נשיא ארה"ב לענייני ביטחון לאומי (APNSA). בסוף החודש, פרסמו ארה"ב ומספר מבעלות בריתה, בהן קנדה, אוסטרליה ובריטניה, הצהרה משותפת בה קראו לקדם פיקוח קפדני בין-לאומי של התפוצה והשימוש לרעה ברוגלות מסחריות.[6]

בד בבד, ב-8 במרץ, פרסם **משרד ראש המודיעין הלאומי** (ODNI) את דו"ח האיומים לשנת 2023 ובמרכזו ההערכה כי במקרה וסין תזהה כי עימות עם ארה"ב מתקרב, קיימת סבירות גבוהה כי היא תוציא לפועל מתקפות סייבר נגד תשתיות חיוניות בארה"ב ונכסיה הצבאיים ברחבי העולם. מתקפות מהסוג הזה עלולות להרתיע את ארה"ב להגיב, מאחר והן עשויות לחבל בתהליכי קבלת ההחלטות במדינה, לעורר בהלה ציבורית בקרב אזרחיה ולשבש את הליכי פריסת כוחותיה הצבאיים בעולם.[7] באותו יום, במסגרת שימוע שנערך בוועדת המודיעין של הסנאט, טען ראש ה-**FBI**, כריסטופר ריי (Christopher Wray), כי המפלגה הקומוניסטית בסין עלולה להשתמש באפליקציית הרשת החברתית TikTok על מנת לאסוף מידע על משתמשיה, לשלוט מרחוק על המכשירים בהם האפליקציה מותקנת או להפיץ דרכם נרטיבים שונים.[8] יממה לפני כן, בשולי וועידת Singapore Defence Technology, טען מפקד **פיקוד הסייבר** וראש סוכנות ה-**NSA**, הגנרל פול נאקאסונה כי האלגוריתמים שבבסיס האפליקציה עלולים לאפשר הפצת מכוונת של מסרים מסוג מסוים, אך לא פירט מעבר לכך.[9]

[5] https://bit.ly/3KjQXaJ ; https://bit.ly/3lmWmEd ; https://on.wsj.com/3n7ACwJ
[6] http://bit.ly/40B8PmT
[7] קישור לדו"ח: https://bit.ly/40gAx84
[8] https://cbsn.ws/3TvrFsQ
[9] https://bit.ly/3no5kl3

נושא נוסף אותו קידם הממשל הוא המעבר לארכיטקטורת רשת המבוססת על עקרונות אפס האמון (Zero Trust). ב-14 במרץ, סוכנות ה-**NSA** פרסמה מסמך, שמטרתו לסייע לבעלי ולמפעילי מערכות מידע ממשלתיות החיונית לביטחון הלאומי (NSS)[10] לשפר את יכולות ניהול הרשאות הגישה (ICAM)[11] שלהן, במטרה לקדם את הטמעת עקרונות אפס האמון, על בסיס עקרונות מסגרת ה-FICAM.[12] המסמך מגדיר רמות בשלות לצורך קידום המעבר בהתאם למרכיבי ה-ICAM.[13] לדוגמא, במרכיב ניהול ההרשאות, רמת המוכנות הבסיסית להטמעת עקרונות אפס האמון דורשת ממשתמשי המערכת להשתמש באמצעי אימות ארגוניים המבוססים על תקנות של NIST,[14] בעוד שרמת מוכנות מתקדמת דורשת ניסוח נהלים לביטול והחלפה מהירה של הרשאות.[15]

לבסוף, החודש פרסם **משרד המבקר הכללי של המחלקה לביטחון המולדת** (OIG),[16] דו"ח שבחן את פעולותיה של **הסוכנות לאבטחת סייבר ותשתיות** (CISA) לאתר ולהתמודד עם אירועי סייבר בעקבות הפריצה ל-SolarWinds, שנחשפה בדצמבר 2020. לפי ממצאי הדו"ח, CISA קיבלה לאחר גילוי הפריצה סמכויות ותקציבים במטרה לשפר את יכולותיה הניהוליות והתפעוליות בהתמודדות עם אירועי סייבר, אך לא גיבשה תכנית עדכנית לגיבוי מערכות התקשורת במקרה של מתקפת סייבר שתשבית את הרשת הראשית. מחברי הדו"ח קראו ל-CISA בין השאר, לפתח מערכת תקשורת ומידע מאובטחת וחלופית לשימוש בחירום ולהעריך מחדש את היקף כוח האדם והמשאבים הנחוצים לטובת פעילותה המבצעית והמודיעינית. כמו כן, על CISA לקבל מסוכנויות פדראליות נוספות מידע על איומי סייבר במסגרת תכנית CDM,[17] וכן עליה לפתח אמצעי אבטחה, כגון Malware NextGen.[18]

---

[10] National Security Systems

[11] Identity, Credential, and Access Management.

[12] Federal Identity, Credential, and Access Management ; הארכיטקטורה מסייעת לסוכנויות פדראליות לנהל את יכולות ה-ICAM.

[13] על פי הרשות לשירותים כלליים (General Services Administration), המעבר לארכיטקטורת אפס אמון נשען על שבעה יסודות: ניהול זהויות והרשאות גישה; הערכת מצב המכשירים המקושרים אליה; הגנה על מידע רגיש מגישה בלתי מורשית באמצעות ניהול הרשת (למשל, באמצעות חלוקה למקטעי משנה); אבטחת יישומים; הפקת תובנות מניתוח התנהלות הרשת בזמן אמת; אוטומציה של תהליכי אבטחה באמצעות תיאום בין יישומי אבטחה שונים; ניהול הגישה למאגרי מידע שונים על סמך סיווגם.

[14] לפירוט, ראו: http://bit.ly/3JVKkKf

[15] https://bit.ly/40aMyw3 ; קישור למסמך: https://bit.ly/3nqbFwE

[16] Office of Inspector General

[17] Continuous Diagnostics and Mitigation ; תכנית שהושקה בשנת 2013, המיועדת לספק שירותי אבטחת סייבר לסוכנויות פדראליות באמצעות הקמת פלטפורמה לאיסוף מידע על איומי אבטחה מכל סוכנות פדראלית. החלק המרכזי בפלטפורמה הוא דשבורד ייעודי הפועל ב-CISA, שאוסף את כלל המידע ומספק תמונת מצב על מידת אבטחת הסייבר בממשל הפדראלי.

[18] בעוד שאנטי-וירוס מסורתי מתמקד בהגנה על נקודת קצה מפני נוזקות, Malware NextGen מתאפיין בניטור איומים מנקודת מבט מערכתית. זאת, באמצעות שימוש באמצעים כמו למידת מכונה וארכיטקטורה מבוססת ענן. https://cnn.it/3Fzo7A7 ; http://bit.ly/3YWUWOl ; קישור לדו"ח המלא: https://bit.ly/3lrMF7y

בקשות תקציב במסגרת חוק ה-NDAA לשנה הפיסקאלית 2024

לאחר פרסום אסטרטגיית אבטחת הסייבר הלאומית, הציג **הבית הלבן** את מסמך בקשת התקציב הממשלתי לשנה הפיסקאלית 2024, ולפיה בכוונת הממשל להקצות 12.7 מיליארד דולר לטובת שדרוג אבטחת הסייבר בקרב סוכנויות הממשל האזרחיות ועוד 13.5 מיליארד דולר יוקצו ל**מחלקת ההגנה** עבור פעילויות בתחום הסייבר.[19]

בקשת התקציב של ה**ממשל הפדראלי** כוללת הקצבה של 3.1 מיליארד דולר עבור **CISA,** סכום הכולל 98 מיליון דולר לטובת אכיפת חוק ה-CIRCIA,[20] לדיווח על תקריות סייבר בקרב תשתיות חיוניות, ו-425 מיליון דולר לטובת פיתוח המערכת החדשה לניתוח נתוני סייבר (CADS),[21] שמטרתה לספק ל-CISA יכולות ניתוח מתקדמות המבוססות על נתונים במרחב הסייבר.

כמו כן, כוללת בקשת התקציב לשנה הפיסקאלית 2024, מספר סעיפים נוספים בתחום אבטחת הסייבר:[22]

- 200 מיליון דולר יוקצו לטובת קרן ה-TMF[23] לחידוש ציוד ומערכות ה-IT הפדראליות ו-63 מיליון דולר מיועדים להרחבת מצבת כוח האדם וכן לתוספת של יכולות איסוף וניתוח מודיעין עבור ה-**FBI**, במטרה לשפר את התמודדותו עם פשיעת סייבר;[24]
- 395 מיליון דולר יוקצו לקידום יוזמות בין-לאומיות בתחום אבטחת הסייבר, בין היתר באמצעות **הלשכה למרחב הסייבר ולמדיניות דיגיטלית** (CDP),[25] שהוקמה באפריל 2022;
- 215 מיליון דולר יועברו ל**מחלקת האוצר** לטובת אבטחת מידע והגנה על מערכותיה וכן במטרה לקדם את המעבר לארכיטקטורת אפס האמון.[26]

בקשת התקציב של **מחלקת ההגנה** לשנה הפיסקאלית 2024 כוללת 145 מיליארד דולר עבור מיזמי מחקר, פיתוח ובחינת פתרונות לשימוש אחראי בטכנולוגיית הבינה המלאכותית ורשתות 5G. מתוך סכום זה, 1.4 מיליארד דולר מיועדים עבור קידום פרויקט מערכת הפיקוד והשליטה הרב ממדית (JADC2)[27] של המחלקה, שמטרתו לחבר בין מערכות נשק ופיקוד ושליטה במרחבי היבשה, הים, האוויר, החלל והסייבר. תחומים נוספים הכלולים בבקשת התקציב של המחלקה מיועדים לסייע לה לסכל תקיפות סייבר מצד יריבותיה של ארה"ב, לרבות קבוצות APT;

---

[19] https://bit.ly/3ndb29o
[20] Cyber Incident Reporting for Critical Infrastructure Act of 2022, החוק נכנס לתוקף במרץ 2022 ומחייב ארגונים מענף התשתיות החיוניות לדווח על אירועי אבטחת סייבר בתוך 72 שעות מזמן גילויים וכן לדווח על ביצוע תשלומי כופר תוך 24 שעות.
[21] Cyber Analytics and Data System
[22] https://wapo.st/3JJibHv
[23] Technology Modernization Fund ; תכנית המיועדת לסייע לסוכנויות פדראליות להשקיע באמצעים טכנולוגיים במטרה לשפר את השירות הניתן לציבור, להתייעל ולהגן על מידע רגיש.
[24] https://bit.ly/425AopH ; קישור למסמך התקציב: https://bit.ly/3mM72MZ
[25] Bureau of Cyberspace and Digital Policy
[26] https://bit.ly/42o6Fsd
[27] Joint All-Domain Command and Control

לקדם את המעבר ליישום ארכיטקטורת אפס האמון; ולשפר את הגנת הסייבר של ספקים וחברות הפועלות בשיתוף עם המגזר הביטחוני.[28] כמו כן, בבקשת התקציב של **פיקוד הסייבר**, ביקש הפיקוד כ-1.1 מיליארד דולר עבור קידום מיזמי מחקר, פיתוח והערכה, לרבות פיתוח ארכיטקטורת לוחמת הסייבר המשותפת (JCWA);[29] ו-129 מיליון דולר עבור רכש והגדלה של מספר צוותי כוח משימת הסייבר (CMF)[30] מ-142 ל-147.[31]

לבסוף, על פי מסמכי הצעת תקציב שפרסם **חיל החלל**, בכוונתו להשקיע בשנים 2024-2028 כשלושה מיליארד דולר עבור פיתוח מערכות תקשורת לוויינית שיהיו חסינות מפני שיבושים (jamming) בזמן מלחמה. פיתוח הלווויינים יסייע לקדם את תכנית PATS,[32] שמטרתה לספק מערך תקשורת לוויינית מאובטחת, על ידי שימוש בלווויינים בעלי הצפנה משופרת המוצבים במסלולי הקפה שונים מחוץ לכדור הארץ. בד בבד, PATS אמורה לספק למפקדי החיל לווויינים בעלי רוחב פס גדול יותר, המותאמים לצרכיהם המבצעיים.[33]

חקיקה

החודש נרשמו יוזמות חקיקה שמטרתן להגביל את המסחר בתחומי הטכנולוגיה, מחשש לפגיעה בביטחון הלאומי האמריקני. ב-7 במרץ, שְׁנֵים-עָשָׂר **מחוקקים** אמריקנים, בראשות הסנאטור הדמוקרטי הבכיר מארק וורנר (Mark Warner) והסנאטור הרפובליקני ג'ון ת'ון (John Thune), הציגו את הצעת החוק הדו-מפלגתית Restricting the Emergence of Security Threats that Risk Information Communications Technology, הקוראת למחלקת המסחר לבחון ובמידת הצורך לאסור, רכישות של סחורות ושירותים מחברות טכנולוגיות זרות, במיוחד מסין. על פי ההצעה, מחלקת המסחר תוסמך לאסור עסקאות לרכש טכנולוגיה הנמצאת בשימוש בקרב תשתיות חיוניות בארה"ב או כוללות מוצרים המעבדים נתונים של למעלה ממיליון משתמשים אמריקנים. כמו כן, תאפשר ההצעה למחלקת המסחר להרחיב את רשימת המדינות הזרות הכלולות בהצעה, וכן עשויה לכלול הגבלות על השימוש ב-TikTok.[34] על רקע זה, הודיעו מספר מדינות מערביות, בהן **בריטניה**, **צרפת**, **הולנד** ו**ניו זילנד** כי יאסרו את השימוש בפלטפורמה הסינית על גבי מכשירים ממשלתיים המשמשים שרי ממשלה, עובדי ציבור,[35] ונציגי פרלמנט.[36]

[28] https://bit.ly/40ujFL7 : קישור למסמך בקשת התקציב של מחלקת ההגנה ; https://bit.ly/3ndb29o ; https://bit.ly/3ZQD6hp
[29] Joint Cyber Warfighting Architecture
[30] Cyber Mission Force teams
[31] https://bit.ly/3ZKYh4i
[32] Protected Anti-Jam Tactical SATCOM
[33] https://bit.ly/3ZajB29
[34] https://bit.ly/3FNiy1a : קישור להצעת החוק ; https://bit.ly/3K0BOeh ; https://bit.ly/3luT8OU
[35] https://bit.ly/3z57bOv
[36] https://reut.rs/3z8Y4MI ; https://reut.rs/3THO06D ; https://bit.ly/3luCSgZ ; https://bit.ly/3ZxpNl7

לצד יוזמות אלו, ב-7 במרץ, אישרה מליאת **בית הנבחרים** את הצעת החוק הדו-מפלגתית Understanding Cybersecurity of Mobile Networks Act, המנחה את מִנְהָלַת התקשורת והמידע הלאומית (NTIA)[37] להגיש לקונגרס דו"ח בנושא הערכת המידה שבה ספקי תקשורת סלולרית נתנו מענה לסיכוני אבטחת סייבר; האופן שבו הטמיעו הספקים שיטות עבודה מומלצות ומסגרות להערכת סיכוני אבטחת סייבר; בנוסף, יכלול הדו"ח מידע בנושא שכיחותם ומידת יעילותם של אלגוריתמים וטכניקות הצפנה ואימות הנמצאים בשימוש בקרב ציוד תקשורת ומכשירים ותוכנות של טלפונים ניידים.[38]

נושא נוסף שקודם החודש בחקיקה הוא הרחבת מיומנויות כוח האדם בשורות הממשל הפדראלי. ב-21 במרץ, הסנאטורית הדמוקרטית ג'קי רוזן (Jacky Rosen) והסנאטורית הרפובליקנית מרשה בלקברן (Marsha Blackburn) הציגו את הצעת החוק The Civilian Cybersecurity Reserve Act המאגדת שתי הצעות חוק, וקוראת לנסח תכניות פיילוט להקמת כוח עתודה סייבר אזרחי במחלקות ההגנה וביטחון המולדת. על פי הצעות החוק, המחלקות יוכלו לגייס מומחי אבטחת סייבר מהמגזר הפרטי, שיסייעו להן לזהות ולהגיב לתקריות סייבר. הצעת החוק הכוללת אושרה במליאת הסנאט בדצמבר 2022, אך טרם הועלתה להצבעה בבית הנבחרים.[39]

צבא וביטחון

החודש המשיכה **מחלקת ההגנה** להשקיע בפיתוח ובהרחבת מצבת כוח האדם המיומן בתחומי הסייבר. ב-1 במרץ, פרסמה המחלקה אסטרטגיה, שמטרתה לצמצם את פער כוח האדם במקצועות הסייבר ברחבי המחלקה ולשפר את הליכי הגיוס, הניהול וההכשרה של עובדים אלו לשנים 2023-2027. באופן ספציפי, האסטרטגיה מתמקדת בזיהוי, ניתוח והערכת פערי כוח האדם במקצועות הסייבר במחלקה מתוך נקודת מבט עכשווית וצופה פני עתיד; פיתוח גישה מקיפה לגיוס, שימור וטיפוח כוח אדם כישרוני בתחומים חיוניים במקצועות הסייבר ובהתאם למשימות המחלקה; הטמעת שינוי תרבותי שמטרתו לייעל את ניהול כוח האדם במחלקה; קידום שיתופי פעולה בין סוכנויות ממשל, התעשייה, האקדמיה ובעלות בריתה של ארה"ב במטרה להרחיב ולשפר את יכולות כוח העבודה בקרב גופי המחלקה.[40]

[37] National Telecommunications and Information Administration
[38] https://bit.ly/3ZOmbMt
[39] https://bit.ly/3zpz3gl ; קישור להצעת החוק הנוגעת למחלקה לביטחון המולדת: https://bit.ly/3nCTqUP
[40] https://bit.ly/3FqtyRM ; http://bit.ly/3LHA3Uz ; קישור למסמך האסטרטגיה: https://bit.ly/3FohzUQ

לצד זאת, החודש המשיך **פיקוד הסייבר** לקדם שינויים במבנה, פעילותו המבצעית וסמכויותיו. ב-2 במרץ, הצהירה מְפַקֶּדת המרכז המשותף למבצעי מודיעין, הכפוף לפיקוד הסייבר,[41] קולונל קנדיס פרוסט (Candice Frost), כי בכוונת הפיקוד להקים מרכז לאיסוף ולשיתוף מודיעין סייבר, שיפעל בדומה למרכזי מודיעין הסייבר הקיימים בפיקודים נוספים בצבא ארה"ב. לדברי פרוסט, המרכז ימוקם בחלקו במרכז הלאומי למודיעין אוויר וחלל (NASIC),[42] יכלול נציגים מה-NSA, מפיקוד הסייבר ומסוכנות המודיעין של מחלקת ההגנה (DIA)[43] ויתמקד באיסוף מודיעין על יכולות הסייבר ההתקפיות של יריבותיה של ארה"ב.[44]

במקביל לכך המשיך צבא ארה"ב לקדם חדשנות ומעבר לשימוש בתוכנה. ב-15 במרץ, השיק **חיל הנחתים** תכנית פיילוט במסגרתה יוקם מפעל תוכנה במתקן של צבא היבשה באוסטין (Austin) שבמדינת טקסס ומטרתו להכשיר נחתים בתחום פיתוח התוכנה. התכנית הושקה כמענה לסביבת ההפעלה העתידית הצפויה של הנחתים, שתחייב אותם להרחיב ולהטמיע את השימוש בפתרונות מבוססי תוכנה בשדה הקרב ללא סיוע מרכזי או מצד ספק אחר. בנוסף, מרכז ההדרכה החדש יעסוק בהכשרת החיילים לטובת פיתוח יישומים מותאמים במהירות עבור מפקדים לצורך ייעול קבלת ההחלטות מבוססת הנתונים. על פי התכנית, עד תום השנה השלישית לפרויקט, יוכשרו 54 נחתים בסך הכל.[45]

במהלך החודש, פרסם עיתון ה-**Washington Post** תחקיר מקיף המבוסס על כ-5,000 מסמכים מודלפים, ולפיו חברת התוכנה הרוסית, NTC Vulkan פיתחה עבור קבוצת ההאקרים Sandworm המזוהה עם המודיעין הצבאי הרוסי (GRU) תוכנה ייעודית, המסייעת לקבוצה לבצע תקיפות סייבר. בנוסף, מתואר בתחקיר פרויקט המכונה בשם Amezit, הכולל, בין היתר, פיתוח מנגנונים להקמה אוטומטית של חשבונות מזויפים ברשתות החברתיות, במטרה להפיץ מידע כוזב בתפוצה המונית. כמו כן, הפרויקט אִפְשֵׁר לגורמים רשמיים ברוסיה לנטר את תנועת הרשת ברחבי המדינה ולקבוע לאילו תכנים ייחשפו המשתמשים.[46]

[41] USCYBERCOM Joint Intelligence Operations Center
[42] National Air and Space Intelligence Center ; יחיה של חיל האוויר העוסקת בניתוח מודיעין על מערכות וכחות אוויר וחלל זרים.
[43] Defense Intelligence Agency
[44] https://bit.ly/3mysULz
[45] http://bit.ly/3LQn0Qv ; http://bit.ly/3JJUMo5 ; http://bit.ly/40kzvbt
[46] https://wapo.st/3lZ0fiO

כמו כן, פיתחה החברה מערכת בשם Scan-V, שמטרתה לאתר חולשות אבטחה פוטנציאליות בשרתים ומערכות ממוחשבות של ארגונים וכן לאסוף מידע על עובדי הארגונים. לבסוף, פיתחה Vulkan את פלטפורמת Crystal-2V, המאפשרת להכשיר קבוצות של עד 30 האקרים לתקוף ארגונים מענפי התשתיות החיוניות.[47]

בנוסף, ב-20 במרץ קרא סגן ראש סגל הממשל הנשיאותי,[48] סרגיי קירייננקו (Sergey Kiriyenko), לאסור על בכירי ממשל רוסיים את השימוש במכשירי אייפון של חברת Apple עד ה-1 באפריל, בשל חשש לאיסוף מודיעין באמצעות המכשירים מצד מדינות מערביות. קירייננקו קרא להשתמש במקומם במכשירים עם מערכות הפעלה חלופיות, כגון Android, חברת Aurora הרוסית או מכשירים של חברות סיניות.[49]

סיכום זירת הסייבר על רקע הפלישה הרוסית לאוקראינה

החודש התפרסמו דו"חות שתיארו מגמות ותחזיות צפויות במסגרת לוחמת הסייבר במלחמה באוקראינה. בנוסף, החלה אוקראינה לקדם חוק שישלב את קבוצת המתנדבים ההאקטיביסטים, צבא ה-IT בשורות הצבא הלאומי.

ב-15 במרץ, פרסמה מיקרוסופט דו"ח במסגרתו סקרו החוקרים תובנות ומגמות בנושא מתקפות הסייבר ומבצעי ההשפעה המיוחסים לרוסיה וכן סיפקו הערכות לקראת המשך הלחימה. על פי הדו"ח, העריכו החוקרים כי רוסיה תוציא לפועל מבצעי השפעה במהלך מערכות הבחירות בפולין, אסטוניה ופינלנד שצפויות להיערך בשנת 2023, מתוך ניסיון לערער את תמיכת נאט"ו והאיחוד האירופי באוקראינה. בנוסף, ציינו החוקרים כי מינואר 2023 החלה קבוצת ההאקרים Sandworm המזוהה עם המודיעין הצבאי של רוסיה לאסוף מל"ם (Reconnaissance) ולהתקין נוזקות Wiper על גבי מטרותיה. לדבריהם, המגמה העלולה להעיד כי הקבוצה נערכת לבצע מתקפות על ארגונים הפועלים מחוץ לשטחה של אוקראינה והחיוניים למאמץ המלחמתי שלה. לבסוף, החוקרים ציינו כי מבצעי ריגול הסייבר המזוהים עם רוסיה צפויים להתמקד בארגונים דיפלומטיים וצבאיים של מדינות חברות ברית נאט"ו, של שכנותיה של אוקראינה ובחברות פרטיות, המהוות חלק משרשרת האספקה הצבאית של אוקראינה.[50]

[47] https://bit.ly/3nUqpUx ; https://bit.ly/43m1sSo
[48] First deputy head of the presidential administration
[49] https://reut.rs/3zhbZAs ; https://bit.ly/3KgZPxv
[50] https://reut.rs/3TEoKOK ; קישור לדו"ח המלא: https://bit.ly/3KeGg9r

בנוסף, ב-8 במרץ השירות הממלכתי לתקשורת מיוחדת ולביטחון מידע של אוקראינה (SSSCIP)[51] פרסם דו"ח ולפיו בחצי השנה הראשונה למלחמה האקרים רוסים הוציאו לפועל תקיפות סייבר במטרה לשבש ולחבל בפעילותו של ענף התקשורת במדינה, כאשר במחציתה השנייה עסקו ההאקרים בריגול סייבר, בגניבת נתונים וכן במבצעי השפעה, והתמקדו במיוחד בענף האנרגיה, בתשתיות חיוניות ואזרחיות ובמוסדות ממשל.[52]

מלבד הדו"חות שהתפרסמו, ב-14 במרץ הודיעה ממשלת אוקראינה על כוונתה לנסח חוק חדש שיסדיר את מעמדה החוקי של קבוצת ההאקטיביסטים המתנדבים, צבא ה-IT וישלב אותה ככוח עתודה פעיל בקנה מידה מלא בצבא אוקראינה.[53]

האיחוד האירופי

על רקע העלייה במספר מתקפות סייבר על ארגונים ציבוריים ופרטיים באירופה בעקבות המלחמה באוקראינה, ב-9 במרץ, פרסמו שרי התקשורת של 27 מדינות ה**איחוד האירופי** הצהרה משותפת, בה ציינו כי על מוסדות האיחוד לגבש תכנית אבטחת סייבר מקיפה, במסגרתה תקים הנציבות האירופית קרן חירום, שתסייע למדינות להתמודד עם מתקפות סייבר. כמו כן, הנציבות, בשיתוף הסוכנות האירופית לאבטחת מידע ורשתות (ENISA) וגופים נוספים, יגבשו המלצות לשיפור חוסנן של התשתיות הדיגיטליות הנמצאות בשטחי האיחוד.[54]

כאמצעי נוסף להיערכות מול איום זה, אישרה **וועדת הפרלמנט האירופי לענייני תעשייה, מחקר ואנרגיה** (ITRE)[55] עדכון עבור פרקי הזמן בהם נדרשים מוסדות האיחוד לדווח על אירועי סייבר: על פי ההנחיות החדשות, המוסדות יחויבו לספק לצוות ה-CERT של האיחוד האירופי דיווח ראשוני על אירוע סייבר שחוו בתוך 24 שעות מגילויו וכן דיווח מפורט, הכולל הערכה של השלכות האירוע, בתוך 72 שעות. כמו כן, יקבל צוות ה-CERT של האיחוד,[56] מימון ותחומי אחריות נוספים ויעסוק בתיאום פעולות לאיתור חולשות אבטחה בקרב מוסדות האיחוד. לצד ה-CERT, תוקם המועצה הבין-מוסדית לאבטחת סייבר (IICB),[57] שתעניק לו הכוונה אסטרטגית וכן תפקח על יישום הוראות אבטחת הסייבר שבמסמך, מצד מוסדות האיחוד.[58]

---

[51] Ukraine's State Service of Special Communications and Information Protection
[52] https://bit.ly/3JyMXRX ; קישור לדו"ח המלא: https://bit.ly/3lsmU6T
[53] https://bit.ly/400i282
[54] https://bit.ly/3ZifFfP
[55] The European Parliament's Committee on Industry, Research and Energy
[56] מכונה גם בתור Cybersecurity Centre או בקיצור CERT-EU.
[57] Interinstitutional Cybersecurity Board
[58] https://bit.ly/3lgOqEo ; קישור למסמך: https://bit.ly/3FwIwWz

לצד יוזמות אלו הגיש האיחוד תכניות עבודה לשנים 2024-2023, המציגות את תקציבו. התכנית הראשונה[59] כוללת הקצאה של 909.5 מיליון אירו (כ-999 מיליון דולר) עבור יוזמות בתחומי הבינה המלאכותית ואבטחת הסייבר. התכנית קוראת להקמה של אקדמיה למקצועות הסייבר, שפעילותה תתמקד בצורכי העסקים הקטנים, הבינוניים והמגזר הציבורי. התכנית השנייה[60] כוללת תקציב ייעודי לשיפור חסינות הסייבר בסך 375 מיליון אירו (כ-412 מיליון דולר), ובמרכזה פיתוח מערכת מתקדמת למעקב ולניתוח של איומי סייבר, על בסיס מרכזי SOC בין-יבשתיים ובאמצעות פיתוח יכולות האבטחה של מדינות.[61] כמו כן, יוקצו תקציבים לעסקים קטנים ובינוניים ולחברות הֶזְנֵק, במטרה לסייע להם לעמוד בדרישות רגולטוריות בתחום אבטחת הסייבר.[62]

לצד מענים אלו, נושא רכש שירותי הענן עמד החודש במרכז העשייה של האיחוד. החודש פרסם **מכון המחקר האירופי לכלכלה פוליטית בין-לאומית** (ECIPE)[63] דו"ח המותח ביקורת על סעיף בהצעת הרגולציה של איחוד האירופי לניהול שירותי ענן (EUCS),[64] המעניקה לספקי שירותי ענן הפועלים בשטחי האיחוד חסינות ממסירת מידע במסגרת חקירות מטעם רשויות אכיפה ממדינות זרות. מחברי הדו"ח הזהירו כי סעיף החסינות עלול לאפשר למדינות האיחוד להדיר ספקיות שירותי ענן אמריקניות[65] משווקי הענן המקומיים מאחר והן מחויבות לציית לחקיקה האמריקנית. מחברי הדו"ח הביעו את חששם שסעיף זה יורחב בעתיד לתחומים טכנולוגיים נוספים, כגון מכשירי IoT, וטכנולוגיות הנמצאות בשימוש בקרב תשתיות חיוניות. כמו כן, הזהירו מחברי הדו"ח כי דרישות לאחסון ועיבוד מידע בשטחי האיחוד האירופי תפגע ביכולתן של חברות אירופיות לקבל שירותי אבטחת סייבר מחברות שאינן אירופיות.[66]

החודש הציגה **CISA** אפליקציית רשת מבוססת קוד פתוח המכונה בשם Decider, שמטרתה לסייע לאנליסטים, מומחי אבטחה וחוקרים למפות את דפוסי פעילותם של האקרים על פי ה-MITRE ATT&CK.

[59] The Digital Europe Programme ; תכנית שהשיקה הנציבות האירופית בשנת 2021, המעניקה מימון לקידום תחומים טכנולוגיים נבחרים באירופה, לרבות בתחום אבטחת הסייבר.
[60] Cybersecurity Work Programme
[61] Cross-border Security Operations Centers
[62] https://bit.ly/3KoGLNY ; קישור לתוכניות: https://bit.ly/42VO32Z
[63] The European Centre for International Political Economy ; מכון מחקר בלגי העוסק בסוגיות הנוגעות למסחר בין-לאומי.
[64] EU Cloud Certification Scheme ; הצעת רגולציה שפרסמה סוכנות אבטחת הסייבר של אירופה (ENISA), המיועדת ליצור התאמה בין סטנדרטים שונים של אבטחת סייבר של שירותי ענן, שנוסחו על ידי מוסדות האיחוד האירופי, גופים בין-לאומיים, המגזר הפרטי ומדינות האיחוד.
[65] המספקות למעלה מ-75% משירותי הענן באירופה.
[66] https://bit.ly/3mKjqNm ; קישור לדו"ח: https://bit.ly/3ySh3Lk

האפליקציה, שפותחה בשיתוף מכון ההנדסה ופיתוח המערכות של המחלקה לביטחון המולדת (HSSEDI)[67] וצוות ה-MITRE ATT&CK, מיועדת לסייע בתהליך המיפוי באמצעות הצגת שאלות על היסטוריית התקיפות של ההאקרים ומאפשרת למשתמשים להתמקד בחלקים הרלוונטיים מתוך ה-MITRE ATT&CK. מטרת המיפוי היא לסייע למשתמשים להשתמש בפונקציות נוספות של MITRE ATT&CK, בהן שיתוף דו"חות מודיעין איומים עם גורמים נוספים או לבחון את הגנת הסייבר שלהם באמצעות דימוי תקיפות.[68]

בד בבד, ב-13 במרץ הודיעה ממשלת **בריטניה** על הקמת הרשות הלאומית לביטחון לאומי (NPSA),[69] אשר תפעל תחת הפיקוח של סוכנות הביון הבריטית MI5. ה-NPSA תספק ייעוץ והדרכה לארגונים ועסקים בהתמודדות עם ריגול תעשייתי, ניסיונות לגניבת נתונים ובהגנה על תשתיות חיוניות לאומיות, טכנולוגיות חדשות ומחקר המהווים איומים על ביטחונה הלאומי של בריטניה. כחלק מכך, ה-NSPA תייעץ לארגונים מקומיים כיצד לנהל את פעילותם העסקית מול חברות סיניות. בנוסף, ה-NSPA עתידה לשתף פעולה עם ה-GCHQ, המרכז הלאומי לאבטחת הסייבר של בריטניה (NCSC) והמשרד הלאומי ללוחמה בטרור (NaCTSO).[70]

כמו כן, החודש פורסמו ממצאים, הדנים בפעילות הסייבר הזדונית המיוחסת ל**סין** במרחב הסייבר בעולם. חוקרים מחברת אבטחת הסייבר SentinelLabs וחברת ה-IT הגרמנית, QGroup GmbH פרסמו הודעה משותפת לפיה זיהו ברבעון הראשון של שנת 2023 שלבי תקיפה ראשוניים נגד ספקיות תקשורת במזרח התיכון המיוחסים לקבוצת ריגול סייבר, שככל הנראה מקושרת לקבוצות הסיניות Gallium ו-APT41. במסגרת תקיפותיהם, ההאקרים פרצו לשרתי Microsoft Exchange בכדי להחדיר Web shells, שאפשרו להם לגנוב הרשאות ומידע. על פי החוקרים, המתקפות שזוהו עשויות להעיד על השתכללות דפוסי התקיפה במסגרת מבצע Operation Soft Cell, במהלכו התמקדו האקרים סיניים בענף התקשורת העולמי החל משנת 2018.[71]

[67] The Homeland Security Systems Engineering and Development Institute
[68] https://bit.ly/3YBAmTz : קישור לאפליקציית הרשת ; https://bit.ly/3M1PcAj https://bit.ly/3JrMySu
[69] National Protective Security Authority
[70] http://bit.ly/3yT45Ne ; https://bit.ly/3JvwxKb ; https://bit.ly/3Ly9Do0 ; National Counter Terrorism Security Office
[71] https://bit.ly/3K6Omj7 : קישור להודעה ; https://bit.ly/3JVkAxy

החודש קידמו ממשל ביידן והקונגרס האמריקני מעני אבטחת סייבר עבור כלל ארגוני התשתיות החיוניות, ביניהם דרישות אבטחה בסיסיות עבור מגזרי המים והחשמל.

ב-3 במרץ, **הסוכנות האמריקנית להגנת הסביבה** (EPA)[72] פרסמה מִזְכָּר, המחייב מדינות בארה"ב להעריך את מידת אבטחת הסייבר של מערכות המים שלהן, כחלק מסקרי התברואה הנערכים בהן.[73] המִזְכָּר, מונה שלוש דרכים לביצוע הביקורת: הערכות פנימיות המתבצעות על ידי מפעילי מתקני המים; הערכה על ידי הממשל ברמת המדינה; והערכה על ידי גורמים חלופיים.[74] בנוסף, מנחה המִזְכָּר את המדינות להעריך את מצב האבטחה של מערכות בקרה תעשייתיות (ICS) במתקני מים וכן מעניק להן את הסמכות לדרוש ממפעילי מערכות אלה לתקן חולשות מהותיות שהתגלו. כמו כן, במקרה בו הערכת אבטחת הסייבר מתבצעת על ידי גוף חלופי, על המדינות לוודא כי היא מתקיימת בתדירות הזהה בה מתקיימים סקרי תברואה (אחת לשלוש או חמש שנים). בד בבד, ה-EPA הציגה במִזְכָּר את הדרכים שעשויות לסייע למדינות לבצע ביקורות אלו, למשל באמצעות קיום הכשרות ייעודיות לעובדים.[75]

במקביל, ב-8 במרץ, נציגת **בית הנבחרים** ג'אן שקובסקי (Jan Schakowsky) והסנאטור אד מרקי (Ed Markey) הציגו את הצעת החוק Water System Threat Preparedness and Resilience Act, שמטרתה להעלות את מודעותם של מפעילי תשתיות מים לאיומי סייבר. ההצעה קוראת ל-EPA לייסד תכנית מענקים בסך 10 מיליון דולר בכל אחת מהשנים הפיסקאליות 2024 ו-2025, שיוקצו למימון הצטרפותם של ארגונים קטנים ממגזר המים למרכז לשיתוף מידע וניתוח של מגזר המים (ISAC Water). כך, יתאפשר לאותם מפעילים הנעדרים המשאבים הנחוצים להצטרף למרכז ולקבל מידע על איומים שעלולים לפגוע בתפקוד מתקניהם.[76]

---

[72] Environmental Protection Agency

[73] Sanitary Surveys ; מדובר בסקרים כלליים הבוחנים את יכולתם של מתקני מים לספק מים נקיים לשימוש.

[74] למשל, הסוכנות לביטחון לאומי של מדינה כלשהי עשויה להעריך את אבטחת הסייבר במתקני מים כחלק מתכנית רחבה יותר לבחינת מצב האבטחה בכלל התשתיות החיוניות.

[75] https://bit.ly/41QtQeo ; קישורים להנחיות: https://bit.ly/3ZrzmCI, http://bit.ly/3LpWAVF

[76] The Water Information Sharing and Analysis Center ; ארגון ללא כוונת רווח, שהוקם בשיתוף ה-EPA ומשמש מסגרת לשיתוף מידע על איומים על מגזר המים בארה"ב. החברות בארגון הינה בתשלום הנע בין 100 ל-7,700 דולר בשנה. https://bit.ly/4040zuY

ב-16 במרץ, **הנציבות האמריקנית הפדראלית לרגולציה על ענף החשמל** (FERC)[77] אישרה את הצעת התאגיד הצפון-אמריקני לאמינות בענף החשמל (NERC)[78] להטמעת תקינת Reliability Standard CIP-003-9, אשר מרחיבה את החובה על מפעילי, בעלי ומשתמשי מערכות חשמל מבוזרות (BES),[79] לנהל סיכוני אבטחת סייבר בשרשראות אספקה של מערכותיהם כך שיחולו גם על רכיבים המוגדרים כבעלי השפעה נמוכה (low impact).[80] טרם אישור ההחלטה, חלה תקינה זו על רכיבים שהוגדרו כבעלי השפעה בינונית וגבוהה בלבד. במסגרת התקינה, שאמורה להיכנס לתוקף באפריל 2026, מפעילי, בעלי ומשתמשי מערכות BES יידרשו לוודא במדיניות אבטחת הסייבר שלהם כי ספקים דואגים לגישה מאובטחת מרחוק למערכות BES. כמו כן, מפעילי מערכות אלו יצטרכו לזהות פעילות זדונית המתבססת על גישה מרחוק של ספקיהם ויוכלו, במידת הצורך, להשבית אותה.[81]

לצד ניסוח הדרישות עבור מפעילי ובעלי תשתיות חיוניות במגזרים הספציפיים, הוביל **ממשל ביידן** מאמצים לקדם את הגנת הסייבר בקרב תשתיות לאומיות חיוניות ברחבי ארה"ב. ב-15 במרץ, המועצה המייעצת לנשיא ארה"ב לענייני מדע וטכנולוגיה (PCAST)[82] הודיעה על הקמת קבוצת עבודה, שתתמקד בגיבוש עקרונות לשיפור מידת חסינות הסייבר של נכסים פיזיים ודיגיטליים בקרב תשתיות חיוניות במדינה. הקבוצה החדשה תקיים במשך כחצי שנה התייעצויות עם מומחים מהמגזר הפרטי, מהממשל ומהאקדמיה, באשר לדרכים בהן ניתן להגן על רכיבים מרכזיים בתשתיות חיוניות מפני מתקפות סייבר, מתקלות בתוכנות ומשיבושים בשרשראות האספקה. גורמים רשמיים בבית הלבן, החברים בקבוצת העבודה, ירכזו את ההצעות המתקבלות מצד המומחים ויתייעצו לגביהן עם גורמי תקינה רשמיים, כגון NIST. לאחר השלמת איסוף ההצעות, יגובשו המלצות שיוגשו לנשיא ארה"ב.[83]

בנוסף, ב-21 במרץ, עדכנה **CISA** את רשימת היעדים הוולונטריים לביצוע (CPG)[84] שמטרתה לסייע לבעלי ומפעילי תשתיות חיוניות להפחית סיכוני אבטחת סייבר.[85] CISA פרסמה את המסמך לאחר קבלת הערות מגורמים בעלי עניין בתחום אבטחת התשתיות החיוניות והוא אורגן לפי חמישה עקרונות כלליים של המסגרת לאבטחת סייבר, שנוסחו על ידי NIST.[86]

---

[77] Federal Electricity Regulatory Commission
[78] North American Electric Reliability Corporation ; NERC הוא גוף רגולטיבי ללא כוונת רווח האחראי לאמינות ובטיחות ולאכיפת תקנים בענף החשמל בארה"ב ובקנדה.
[79] Bulk Electric System ; מערכת חשמל הכוללת אתרים לייצור חשמל, קווי הולכה ומערכות הבקרה שלהם.
[80] רכיבי BES מסווגים לשלוש רמות: ברמה הגבוהה נמצאות מערכות המוגדרות כבעלות השפעה גבוהה, הנמצאות בדרך כלל ברמת מרכז הבקרה. מערכות המוגדרות כבעלות השפעה נמוכה הן מערכות שאינן מוגדרות כמערכות הממלאות תפקידים חיוניים בתפקוד ה-BES.
[81] https://bit.ly/3nvIAjl ; https://bit.ly/3TKFzHI
[82] The President's Council of Advisors on Science and Technology
[83] https://bit.ly/3LQSPsq ; קישור להודעת המועצה: https://bit.ly/3z6e2Hs
[84] Cross-Sector Cybersecurity Performance Goals
[85] הגרסה האחרונה של המסמך פורסמה באוקטובר 2022. במקור, המסמך פורסם בהתאם לתזכיר נשיאותי מיולי 2021, המנחה את CISA ו-NIST לנסח רשימת יעדים לביצוע באבטחת סייבר של תשתיות חיוניות. קישור לתזכיר: https://bit.ly/3npraog
[86] חמשת העקרונות הם: זיהוי ; הגנה ; איתור ; תגובה וחזרה לשגרה.

המסמך כולל המלצות פעולה שמטרתן לסייע לארגונים מענפי התשתיות החיוניות ליישם את חמשת העקרונות וכן לגבש תכניות אבטחת סייבר מקיפות ומותאמות. בנושא המעקב, לדוגמה, על כל ארגון להחזיק ברשימה הכוללת את איומי הסייבר הרלוונטיים לו וכן להגדיר כללי מעקב ואמצעי התראה טכנולוגיים מתאימים. בד בבד, על כל ארגון לקבוע מראש את הגופים הרלוונטיים להם הוא נדרש לדווח על אירועי סייבר, ברמה הפדראלית והמדינתית.[87]

כמו כן, **המועצה האמריקנית הלאומית לייעוץ לענייני תשתיות חיוניות** (NIAC)[88] פרסמה דו"ח העוסק בהסרת חסמים במטרה לקדם שיתופי פעולה בין ארגונים מענפי התשתיות הלאומיות, המגזר הפרטי והמגזר הציבורי, על מנת להגן עליהם מאיומים, לרבות איומי סייבר. מחברי הדו"ח קראו להטיל דרישות אבטחת סייבר מחייבות על כלל הספקים המפתחים את החומרה והתוכנה הנחוצות לגופי תשתיות חיוניות. כמו כן, הדגישו חברי המועצה את הצורך להעדיף פיתוח תקני אבטחה במספר תחומים מוגדרים, בהם מִדּוּל איומים (Threat modeling) וחלוקת רשתות לקטעים (segmentation). בנוסף, ציינו מחברי הדו"ח את הצורך לשפר את שיתוף מודיעין איומי הסייבר והמליצו להקים קבוצה שתאגד מגזרים שונים ותנסח תגובות מתואמות לתקריות סייבר. בנוסף, המחברים ציינו את דירקטיבת NIS2 של האיחוד האירופי כמודל לתקנות שיש לנסח בתחום ההגנה על תשתיות חיוניות.[89]

לבסוף, ב**אוסטרליה**, הודיע מזכיר מחלקת הפנים, מייקל פזולו (Michael Pezzullo), במהלך החודש כי ב-1 במאי 2023 תוקם במחלקה קבוצת עבודה חדשה לענייני אבטחת סייבר ותשתיות (CISG),[90] שתהיה אחראית על יישום אסטרטגיית אבטחת סייבר לאומית חדשה, שדבר פיתוחה על ידי הממשלה פורסם בדצמבר 2022. בד בבד, CISG תהיה אחראית על ייסוד שיתופי פעולה בין הממשל למגזר הפרטי במטרה לשפר את חוסנן של תשתיות לאומיות מפני מתקפות סייבר, קיום תרגילי אבטחה ותגובה לאירועי סייבר בשיתוף מִתְאֵם חדש לענייני אבטחת סייבר, שטרם מונה.[91]

[87] https://bit.ly/3lGRppM ; קישור למסמך, הכולל את כלל משימות המשנה ליישום חמשת העקרונות: https://bit.ly/42JeKaW
[88] National Infrastructure Advisory Council; מועצה פדראלית המייעצת לנשיא ארה״ב, דרך המחלקה לביטחון המולדת בהגנה על תשתיות חיוניות ושירותים לשעת חירום מאיומים שונים - במרחב הפיזי ובמרחב הסייבר.
[89] https://bit.ly/3FsSsAy ; קישור לדו״ח: https://bit.ly/3Tw8wY8
[90] Cyber and Infrastructure Security Group
[91] https://bit.ly/3m1jQ1U

החודש גורמים ב**ממשל האמריקני** חשפו פרטים על המאמצים המתגבשים להגן על מגזר האנרגיה מאיומי סייבר. ב-8 במרץ, ציין מנהל המשרד לאבטחת סייבר, אבטחת אנרגיה ותגובה למצבי חירום (CESER)[92] הכפוף למחלקת האנרגיה, פואש קומאר (Puesh Kumar), כי המעבדה הלאומית של מחלקת האנרגיה לאנרגיות מתחדשות (NREL)[93] בוחנת סיכוני אבטחת סייבר על מערכות לאספקת חשמל וכן מחברת דו"ח המסכם את ממצאי הבדיקה. באותו ראיון, ציינה מנהלת מערכות המידע של מחלקת האנרגיה, אן דאנקין (Ann Dunkin), כי המחלקה קרובה לסיום גיבוש אסטרטגיית אבטחת סייבר חדשה שתתמקד בפיתוח הגנה מקיפה על תשתיות אנרגיה חיוניות, בשיתוף המגזר הפרטי ושותפים בין-לאומיים.[94]

החודש הציגו מחוקקים וארגונים ללא כוונת רווח יוזמות שמטרתן להעריך את סיכוני אבטחת הסייבר שמקורם בספקי צד שלישי. ב-23 במרץ, יושב ראש וועדת **הסנאט האמריקני** לביטחון המולדת ועניינים ממשלתיים, גארי פיטרס (Gary Peters) והסנאטור ג'וש האולי (Josh Hawley) הציגו בשנית את הצעת החוק הדו-מפלגתית The Securing Open Source Software Act.[95] ההצעה מנחה את CISA לנסח מסגרת להערכת סיכונים, ומטרתה להעריך את אופן השימוש של הממשל הפדראלי וכן של בעלי ומפעילי מתקני תשתיות חיוניות בתוכנות המבוססות על קוד פתוח וכן להעסיק מומחי תוכנה להתמודדות עם תקריות סייבר שמקורן בחולשות תוכנה. בנוסף, מנחה הצעת החוק את המשרד האמריקני לניהול ולתקציב (OMB)[96] לפרסם הנחיות שיסייעו לממשל הפדראלי להשתמש בתוכנות באופן בטוח.[97]

---

[92] Office of Cybersecurity, Energy Security and Emergency Response; משרד ה-CESER הוא הגוף האחראי לאבטחת הסייבר ולאבטחה הפיזית של תשתיות החשמל והאנרגיה בארה"ב.
[93] The National Renewable Energy Laboratory
[94] https://bit.ly/3FL8ZzJ
[95] ההצעה הוצגה לראשונה בסנאט בספטמבר 2022.
[96] Office of Management and Budget
[97] CISA's Cybersecurity Advisory Committee; וועדת מומחים שהוקמה בדצמבר 2021 ומיועדת לסייע ל-CISA לזהות, להעריך ולהגיב לאיומי סייבר; https://bit.ly/40qCnDF

כמו כן, הציג תאגיד **MITRE** אב-טיפוס לאפליקציית רשת בשם RMM,[98] המציגה ומסייעת למשתמשים להטמיע את מסגרת ה-SoT,[99] שניסח התאגיד על מנת להגדיר ולתת מענה לסיכונים שמקורם בשרשרת האספקה. מטרת האפליקציה לסייע לצוותי אבטחת סייבר להגדיר, להעריך ולְכַמֵּת סיכוני אבטחה בשרשראות אספקה, שמקורם בספקי שירותים, תוכנה וקושחה.[100] כמו כן, האפליקציה תאפשר למשתמשי ה-SoT להציג, להתאים אישית ולשתף את המידע עם מקורות חיצוניים, במטרה לתת מענה לאיומי אבטחה ארגוניים.[101]

כחלק מהדגש הגובר של ה**ממשל האמריקני** על נושא ההתמודדות עם מתקפות כופרה, ב-9 במרץ הודיעה CISA על השקתה הרשמית של תכנית ה-RVWP,[102] שמטרתה להתריע בפני מפעילי תשתיות חיוניות על חולשות במערכותיהם ובכך למזער את ההסתברות למתקפות כופרה מוצלחות על תשתיות חיוניות. במסגרת התכנית, שהושקה ב-30 בינואר 2023 לפי חוק ה-CIRCIA, הזהירה הסוכנות 93 ארגונים מפני חולשות ה-ProxyNotShell בשרתי Microsoft Exchange.[103] השקת תכנית ה-RVWP תואמה באמצעות כוח המשימה המשותף ל-CISA ול-FBI למאבק במתקפות כופרה (JRTF),[104] שהושק בספטמבר 2022.[105]

על רקע איומי הסייבר הגדלים על גופים מענף הפיננסים והבנקאות ברחבי העולם, ב-9 במרץ, ראש מועצת הביקורת **בבנק האירופי המרכזי** (ECB),[106] אנדריאה אנריה (Andrea Enria), אמר כי ה-ECB עתיד להגביר את התמקדותו בנושא אבטחת הסייבר ותשתיות ה-IT של בנקים באירופה.

---

[98] Risk Model Manager
[99] System of Trust
[100] SoT מספקת למשתמשיה מידע על טיפול בחולשות אבטחה בשרשראות אספקה על בסיס ידע המגיע ממספר מקורות, בהם ארגוני תקינה ו-MITRE.
[101] https://bit.ly/40LChq0 ; https://bit.ly/3JUKEZv
[102] Ransomware Vulnerability Warning Pilot
[103] החולשות, שפורסמו על ידי מיקרוסופט בספטמבר 2022, עלולות לאפשר לתוקפים ליישם ביצוע קוד מרחוק (remote code execution) בשרתי Exchange.
[104] Joint Ransomware Task Force
[105] https://bit.ly/3mT0Y5n
[106] European Central Bank

אנריה ציין כי בכוונת ה-ECB להשיק במהלך שנת 2024 תהליך לבחינת היכולת של בנקים באירופה להתמודד עם תקריות סייבר ולשוב לשגרה באמצעות קיום תרגילי דימוי תקיפות.[107]

בד בבד, **הממשל האמריקני** הוביל החודש את נושא הטמעת דרישות האבטחה המינימליות בקרב גופי ענף הפיננסים. ב-15 מרץ, פרסמה הנציבות האמריקנית לניירות ערך (SEC) לתגובות הציבור הצעה לכללים חדשים, שמטרתם להנחות גופים החיוניים למסחר בניירות ערך, כיצד לשפר את מידת אבטחת הסייבר שלהם. על פי ההוראות, על גופים שחוו אירועי סייבר לדווח עליהם ל-SEC באופן מיידי באמצעות טופס ייעודי מקוון, וכן עליהם לדווח על הפעולות שנקטו במסגרת התגובה לתקריות וההמשכיות העסקית. בנוסף, גורמים העוסקים בסחר וניהול ניירות ערך יידרשו ליישם תכניות למעקב ולהתמודדות עם גישה בלתי מורשית למידע הנמצא ברשותם וכן ליידע לקוחות שנפגעו בעקבות אירועים אלו בטווח של עד 30 יום מרגע גילוי התקרית.[108]

ב-7 במרץ, הודיע סגן מזכיר **מחלקת המסחר האמריקנית**, דון גרייבס (Don Graves), על השקת קהילת אבטחת סייבר לענייני עסקים קטנים.[109] הקהילה תשויך למרכז הלאומי למצוינות באבטחת סייבר (NCCoE)[110] הכפוף ל-NIST ותסייע לעסקים קטנים, כולל עסקים המספקים שירותי אבטחה, לשפר את מידת אבטחת הסייבר שלהם. בנוסף, קראה המחלקה להעברת חלק מאחריות אבטחת הסייבר מהצרכנים והעסקים הקטנים, לספקיות התוכנה הגדולות. לדברי גרייבס, הקמת הקהילה תאפשר ל-NIST לוודא כי ההנחיות המתפרסמות על ידו אכן מיושמות על ידי עסקים קטנים.[111] מלבד עסקים קטנים, תכלול הקהילה גם אגודות מסחר וגורמים נוספים, שיוכלו לספק ל-NIST תובנות בנושא שיפור אבטחת הסייבר שלהם.[112]

בד בבד, ב-21 במרץ, ה**מרכז הלאומי לאבטחת סייבר של בריטניה** (NCSC) השיק את שירות ה- The Cyber Action Plan, במסגרתו עסקים קטנים מקבלים עצות לשיפור מידת אבטחת הסייבר שלהם המבוססות על קווים מנחים מאת ה-NCSC, בהתאם לפרטים שהם ממלאים באופן מקוון על מאפייני האבטחה שלהם.

---

[107] https://bit.ly/3ZYGczH ; https://bit.ly/3YNVV3d
[108] https://bit.ly/3ncunHO https://reut.rs/3nglQ6R ; קישור למסמך המציג את עיקרי ההחלטה: https://bit.ly/40atoX4
[109] Small Business Cybersecurity Community of Interest
[110] National Cybersecurity Center of Excellence
[111] https://bit.ly/3J4gxyt
[112] https://bit.ly/3L65I1y ; https://bit.ly/3JVuD75

בנוסף, הושק השירות Check your Cyber Security המאפשר לארגונים קטנים, בהם בתי ספר ומוסדות צדקה, לזהות ולתקן חולשות במערכות החשופות ברשת. השירותים ניתנים כחלק מתכנית הגנת הסייבר האקטיבית (ACD),[113] שמטרתה להגן על עסקים ועל הציבור בבריטניה מפני איומי סייבר נפוצים.[114]

בעקבות המגמה הגוברת של הטמעה ושילוב שירותים דיגיטליים בקרב מערכות הבריאות בעולם, החודש פרסמו מספר מדינות תכניות בנושא ניהול סיכוני סייבר במגזר הבריאות וההגנה על מידע רפואי. ב-7 במרץ, ה-**NCCoE** פרסם לתגובות הציבור טיוטת מסמך בנושא שיפור מידת אבטחת הסייבר בתהליכי אחסון וניהול נתונים ומידע גנטי, החיוניים למחקר הרפואי ולשימור מעמדה הטכנולוגי של ארה"ב. מחברי הדו"ח ציינו כי מידע מסוג זה אינו מאובטח באופן נאות והציגו לכן מספר פתרונות אפשריים להערכת הציבור, בהם שימוש במערכת פרטיות דיפרנציאלית (DF)[115] המאפשרת אנונימיזציה של פרטים מזהים והצפנה הומומורפית מלאה (FHE).[116]

כמו כן, ב-10 במרץ, ה**מחלקה האמריקנית לבריאות ושירותי האנוש**, בשיתוף המועצה המתאמת במגזר הבריאות (HSCC),[117] פרסמה מסמך שמטרתו לסייע לארגוני בריאות להתאים את תכניות אבטחת הסייבר שלהם אל עקרונות מסגרת אבטחת הסייבר של NIST,[118] על ידי שיפור ההליכים באמצעותם ארגוני בריאות מבצעים ניהול סיכוני אבטחת סייבר. על פי המדריך, יישום המסגרת יאפשר לארגוני בריאות לפתח שפה משותפת, באמצעותה יוכלו לדון, בשיתוף לקוחות, שותפים עסקיים וארגוני ממשל, בסיכוני הסייבר ובדרכים להתמודד עימם. כמו כן, יישום עקרונות המסמך עשוי לסייע לארגוני בריאות לזהות את העקרונות והתקנים היעילים ביותר עבורם לניהול סיכוני אבטחה, בהתאם לצורכיהם הייחודיים.[119]

בד בבד, ב-30 במרץ, **המִנְהָל האמריקני למזון ולתרופות** (FDA) פרסם מסמך, המחייב את כלל יצרני המכשור הרפואי להגיש ל-FDA תכניות לניטור, לזיהוי ולהתמודדות עם חולשות אבטחה וכן לבצע עדכוני אבטחה באופן שוטף.

---

[113] Active Cyber Defence
[114] קישור לשירות ה-The Cyber Action Plan: https://bit.ly/3yXPkZG ; קישור לשירות ה-Check your Cyber Security: https://bit.ly/3FMapu1 ; https://bit.ly/3yXhjsz
[115] Differential privacy ; מסגרת המאפשרת לנתח דפוסים בתוך מאגרי מידע, תוך הימנעות מחשיפת מידע פרטי אישי.
[116] Fully Homomorphic Encryption ; שיטת הצפנה המאפשרת לעבד מידע מוצפן מבלי לפענחו. שיטת הצפנה זו מאפשרת למעשה לעבד מידע גם בסביבה שעלולה להיות חשופה למתקפות של גורמים זדוניים ; https://bit.ly/3JnVLv8 ; קישור לטיוטת המסמך: https://bit.ly/3JswujB
[117] The Health Sector Coordinating Council ; מועצה המייצגת למגזרי משנה של מערכת הבריאות בארה"ב, המשתפת פעולה עם מחלקת הבריאות בשיפור המוכנות לאיומי סייבר ואיומים פיזיים המשפיעים על המערכת.
[118] https://bit.ly/2zMAUjx
[119] https://bit.ly/3mQ4rSe https://bit.ly/3LGf0BO ; קישור למסמך: https://bit.ly/3Fmjh9x

בנוסף, המסמך מחייב יצרני מכשור רפואי לספק ל-FDA רשימת רכיבים ותוכנה (SBOM)[120] של מכשור רפואי. הצגת הנהלים החדשים נעשתה במסגרת חוק התקציב הפדראלי לשנת 2023,[121] המנחה את ה-FDA לעדכן את הנחיות אבטחת הסייבר של מכשור רפואי, לפחות אחת לשנתיים.[122]

לבסוף, החודש פרסמה **מחלקת הבריאות והרווחה של בריטניה** (DHSC)[123] אסטרטגיה חדשה שמטרתה לשפר את ההתמודדות של מגזר הבריאות עם איומי סייבר וכן לשפר את חסינות הסייבר של שירות הבריאות הלאומי של בריטניה (NHS), עד לשנת 2030. האסטרטגיה כוללת חמישה עוגנים מרכזיים, בהם זיהוי תחומים ומערכות במגזר הבריאות שתקיפתם עלולה לגרום למידת הנזק המרבי למטופלים; איגום משאבים, מיומנויות ויכולות קיימות על פני מגזר הבריאות במטרה לשפר את זמן התגובה לתקריות סייבר ועל מנת למזער נזקים פוטנציאליים; הרחבת מצבת כוח האדם המיומן במקצועות הסייבר וקידום הכשרה בסיסית בתחום הסייבר עבור כלל העובדים; הטמעת אמצעי אבטחה בקרב מערכות קיימות ובטכנולוגיות חדשות במגזר הבריאות; ותמיכה בכלל הארגונים מענף הבריאות בהפחתת ההשפעות של תקריות סייבר וזמן ההתאוששות מהן ושמירה על תפקודם של השירותים החיוניים ביותר. המחלקה ציינה כי במהלך קיץ 2023 תפרסם תכנית יישום מלאה של האסטרטגיה, שתכלול צעדים מפורטים ותגדיר מדדים שישמשו כאמות מידה להערכת מידת חסינות הסייבר של גופים מענף הבריאות במהלך שלוש השנים הקרובות.[124]

החודש פרסמה **ENISA** את דו"ח איומי הסייבר הראשון שלה, בו הזהירו המחברים כי החפיפה ההולכת וגדלה בין סביבות IT ו-OT והשכיחות הגוברת של חולשות אבטחה במערכות ICS עלולות לעודד קבוצות כופרה לשבש את תפקודן של תשתיות מענפי התעופה, הימאות, הרכבות והתעבורה. על פי המחברים, פושעי סייבר אחראים למרבית התקיפות שנרשמו על ארגונים מענפי התחבורה (54%), וכן כי מאז הפלישה הרוסית לאוקראינה נרשמה עלייה בפעילותם של האקטיביסטים באירופה. לבסוף, המחברים ציינו כי מתוך ענפי התחבורה, מגזר התעופה חווה את מרבית תקיפות הסייבר (28%).[125]

---

120 Software Bill of Materials
121 The Consolidated Appropriations Act
122 https://cnn.it/3G9ULZw https://bit.ly/3Gcc2RI ; קישור למסמך: https://bit.ly/40MiYx6
123 Department of Health and Social Care
124 https://bit.ly/3z1TeRi ; קישור לאסטרטגיה המלאה: https://bit.ly/3z12hC7
125 ענף התעבורה חווה 24% מהתקיפות, מגזר הרכבות 21% ומגזר הימאות 18%. http://bit.ly/3JKS0Pf ; הקישור לדו"ח: http://bit.ly/3LZ9oml ; http://bit.ly/3LP6i49

ב-7 במרץ, פרסמה ה**רשות האמריקנית לאבטחת התחבורה** (TSA)[126] דרישות אבטחת סייבר חדשות המחייבות מפעילי נמלי תעופה ומטוסים הנמצאים תחת פיקוח הרשות לנסח תכנית לשיפור חסינות הסייבר במטרה למנוע פגיעה בתשתיות חיוניות במגזר התעופה. על פי הדירקטיבה, על מפעילי נמלי תעופה וחברות תעופה להטמיע אמצעים למניעת גישה בלתי מורשית למערכות חיוניות וכן לפצל את רשתותיהם למקטעים (segmentation), על מנת להגן על המשך פעילותן של מערכות OT במקרה של תקיפת מערכות IT. בנוסף, על מפעילי התשתיות ליישם מדיניות לזיהוי אנומליות ולאיתור איומי סייבר, וכן להתקין עדכוני אבטחה במערכות הפעלה, יישומים, מנהלי התקנים וקושחה.[127]

החודש המשיכה סינגפור במאמצים לשמר את מעמדה כמרכז ימי גלובלי מוביל. ב-3 במרץ, **רשות הימאות והנמלים** במדינה (MPA)[128] פרסמה הודעה, בה הציגה תכנית להקים עד לשנת 2025 את המרכז לאבטחת סייבר ותפעול ימי (MCAOC),[129] שתפקידו לנטר אחר איומי סייבר ולהתריע עליהם בזמן אמת. בנוסף, ה-MCAOC יספק המלצות בנושא שחזור מערכות וחזרה לשגרה בעקבות אירועי סייבר וכן יקל על שיתופי מידע בין מפעילי מסופים בנמלים וקווי תעבורה ימיים. כמו כן, המרכז יספק למומחי אבטחה במגזר הימאות הכשרה ופלטפורמה לתרגילי דימוי תקיפה ויעודד ארגונים בענף לאגד משאבים פיננסיים וכוח אדם לצורך התמודדות עם איומי סייבר.[130]

[126] Transportation Security Administration
[127] http://bit.ly/3mJtQwI; https://bit.ly/41dc045
[128] Maritime and Port Authority
[129] The Maritime Cyber Assurance and Operations Centre
[130] https://bit.ly/3Zjrjai

בד בבד, פרסמה נציבות ה-**Cyberspace Solarium** האמריקנית, הפועלת כארגון ללא כוונת רווח, דו"ח בו המליצה על הקמת מעבדה שתבחן את מידת חסינות הסייבר וחולשות האבטחה בקרב מערכות OT חיוניות במגזר הימאות באמצעות בחינת שרשראות האספקה שלהן. המעבדה תוקם על ידי משמר החופים והמרכז הלאומי להדמיה וניתוח לענייני תשתיות של CISA (NISAC)[131] ובשיתוף המגזר הפרטי. כמו כן, המליצו מחברי הדו"ח למשמר החופים לשפר את הכשרת כוח האדם המיומן במקצועות אבטחת הסייבר, לרבות באמצעות ניסוח תכנית לגיוס כוח אדם מהמגזר הפרטי, לפרקי זמן מוגדרים.[132]

ב-30 במרץ, **משרד ראש הסייבר הלאומי האמריקני** (ONCD) ומועצת החלל הלאומית[133] הודיעו כי בכוונת ה-ONCD לכנס במהלך 2023 סדנאות עבודה ברחבי ארה"ב בהשתתפות נציגים מהמגזר הפרטי, על מנת לקבל משוב ותובנות מהתעשייה בנושא אבטחת הסייבר של מערכות חלל ולהציג פערים ברגולציה הקיימת. בנוסף, מחלקת המסחר האמריקנית תקיים במועד שטרם נקבע סימפוזיון בנושא אבטחת סייבר של מערכות חלל, בהשתתפות גורמי מפתח מהממשל הפדראלי ותעשיית החלל. לבסוף, הודיעו משרד ה-ONCD, מועצת החלל הלאומית, גורמי ממשל נוספים וגורמים בכירים מתעשיית החלל כי NIST צפוי להשלים במהלך השנה הפיסקאלית 2023 דו"ח, שיתמקד באבטחת סייבר במסגרת פעילות לוויינים מסחריים ויקדם את הטמעת מסגרת אבטחת הסייבר (NIST CSF)[134] בקרב גופי מגזר החלל.[135]

[131] CISA's National Infrastructure Simulation and Analysis Center
[132] https://bit.ly/3Ko1WyL ; קישור לדו"ח: https://bit.ly/3zqt2jG
[133] National Space Council
[134] NIST Cybersecurity Framework
[135] https://bit.ly/3nD3I7d

כצעד תומך באסטרטגיית אבטחת הסייבר הלאומית של **ארה"ב**, ב-8 במרץ פרסם משרד המבקר הממשלתי (GAO) מסמך העוסק באתגרים הניצבים בפני מקבלי ההחלטות בקידום המעבר לפתרונות מבוססי הצפנה פוסט-קוונטית. המסמך מתייחס לקושי בגיוס והכשרת כוח אדם מיומן בתחומי ההצפנה ואבטחת מאגרי מידע; למשך הזמן הארוך הנדרש לשדרוג מערכות מידע שיתמכו בהצפנה פוסט-קוונטית והמחזיקות בנתונים רגישים; ולצעדים שניתן ליישם כנגד פענוח ההצפנה של מידע רגיש.[136]

במקביל, ב-15 במרץ, **המחלקה למדע, חדשנות וטכנולוגיה של ממשלת בריטניה** (DSIT)[137] פרסמה אסטרטגיה לאומית שמטרתה להפוך את בריטניה למובילה עולמית בתחומי המדע וההנדסה הקוונטיים; להגדיל את חלקה בפעילות הכלכלית העולמית בנושא מחקר ופיתוח של טכנולוגיות קוונטיות ולהפוך אותה ליעד מועדף עבור משקיעים וכישרונות מרחבי העולם; לקדם את הטמעת השימוש בטכנולוגיות קוונטיות לטובת הכלכלה, החברה והביטחון הלאומי של בריטניה; ולהטמיע רגולציה לאומית ובין-לאומית שתעודד חדשנות ושימוש אתי בטכנולוגיות קוונטיות. לטובת יישום היעדים, בכוונת הממשלה להקצות 2.5 מיליארד ליש"ט (כשלושה מיליארד דולר) עד לשנת 2034.[138]

על רקע השיח הגובר בעולם על השלכות השימוש באפליקציות מבוססות טכנולוגיית הבינה המלאכותית, ב-15 במרץ הודיעה מְנַהֶלֶת המידע הראשית של **הקרן האמריקנית הלאומית למדע** (NSF),[139] דורותי ארונסון (Dorothy Aronson), כי ה-NSF החלה בהקמת מערך מקרי בוחן, שיביאו לידי ביטוי את היתרונות והחסרונות בשימוש בצ'טבוטים מבוססי טכנולוגיית הבינה המלאכותית, כגון ChatGPT. כמו כן, הודיעה ארונסון כי ה-NSF מגבשת עקרונות, לפיהם גופי ממשל יוכלו להשתמש בצ'טבוטים בצורה מבוקרת.[140]

---

[136] https://bit.ly/3JGjw0r ; קישור למסמך: https://bit.ly/3JDQCy3
[137] Department for Science, Innovation and Technology
[138] https://bit.ly/3mKYNR9 ; קישור למסמך האסטרטגיה: https://bit.ly/3n0vM3Z
[139] National Science Foundation
[140] https://bit.ly/3nd2zTR

בנוסף, ב-9 במרץ, **לשכת המסחר של ארה"ב** (USCC)[141] המהווה את קבוצת הַשַּׁדְלָנוּת הגדולה במדינה, פרסמה דו"ח במסגרתו קראה לקובעי המדיניות לקדם את הסדרת השימוש בטכנולוגיית הבינה המלאכותית וכן לנסח כללים וחוקים שמטרתם לוודא כי הפיתוח והפריסה של טכנולוגיית הבינה המלאכותית ייעשו באופן אחראי. כמו כן, קראו המחברים לטפח באמצעות חינוך והכשרה כוח אדם שיהיה מיומן להשתמש בבינה מלאכותית במגזר הממשלתי והפרטי; לקדם שיתופי פעולה עם מדינות ובעלות בריתה של ארה"ב בניסוח כללים ונורמות התנהגות ועוד.[142]

לבסוף, ב**בריטניה**, פרסמה ב-29 במרץ המחלקה למדע, חדשנות וטכנולוגיה אסטרטגיה הקוראת לגופי רגולציה במדינה לנסח תקנות הנוגעות לפיתוח ולשימוש בטכנולוגיית הבינה המלאכותית על פי חמשת העקרונות הבאים: בטיחות ואבטחה; שקיפות ובהירות; שימוש בבינה מלאכותית באופן הוגן ושאיננו פוגעני; פיקוח יעיל על שימוש בבינה מלאכותית; יכולת לערער על החלטות מזיקות של מערכות מבוססות בינה מלאכותית.[143]

בעקבות מתקפת הסייבר על אתרים ממשלתיים ב**אלבניה** שאירעה ביולי 2022 ויוחסה להאקרים איראניים, ב-24 במרץ הודיע **פיקוד הסייבר האמריקני** כי ניהל מבצע Hunt Forward בשיתוף עם גורמים בממשלת אלבניה, במהלכו פעלו לאתר איומי סייבר ולזהות חולשות במערכות ממשלתיות ותשתיות חיוניות במדינה. המבצע התנהל במשך שלושה חודשים ואִפְשֵׁר לממשלת אלבניה לאסוף תובנות במטרה לשפר את הגנת הסייבר הלאומית, וכן סיפק לממשלת ארה"ב מידע על הטכניקות, הטקטיקות ושיטות הפעולה (TTPs) של איראן במרחב הסייבר.[144] שיתוף הפעולה נרשם כחלק מסיוע בסך 50 מיליון דולר שאישר ממשל ביידן בפברואר 2023 ומטרתו לשפר את הגנת הסייבר של אלבניה.[145]

---

[141] The United States Chamber of Commerce
[142] https://reut.rs/3lopmv8 ; קישור לדו"ח: https://bit.ly/3JQXtp2
[143] https://bit.ly/3K8IyFJ ; קישור למסמך האסטרטגיה: https://bit.ly/3Kt9f9v
[144] https://bit.ly/3KiYqqz ; https://bit.ly/3M2GfGU
[145] http://bit.ly/3zs4Ltt

לבסוף, ב-29 במרץ הודיעה שגרירות ארה"ב בסן חוזה (San José) כי מחלקת המדינה האמריקנית תעניק לבקשת **קוסטה ריקה** סיוע בסך כ-25 מיליון דולר במטרה לממן הכשרות, התקנת תוכנות וחומרות מאובטחות, וכן במטרה להקים מרכז SOC חדש שיסייע ביכולות ניטור, מניעה ותגובה למתקפות סייבר, בין השאר על המגזר הממשלתי וענף התשתיות החיוניות. כמו כן, עשויה קוסטה ריקה להצטרף לכוח המשימה המשותף למאבק במתקפות כופרה (JRTF).[146] הממשל האמריקני אישר את הסיוע על רקע מתקפות הכופרה שחוותה קוסטה ריקה באפריל 2022.[147]

[146] https://bit.ly/3Kp5HVA ; https://bit.ly/3lUcldf
[147] https://bit.ly/40BHKA5