"ארגז הכלים" של האיחוד האירופי כחלק מדיפלומטיית הסייבר

אָנֶגְרֶט בֶּנדְיֶיק

בספטמבר 2017 עדכן האיחוד האירופי את אסטרטגיית ביטחון הסייבר שלו משנת 2013. הגרסה החדשה נועדה לשפר את ההגנה על התשתיות הקריטיות של אירופה ולהעצים את האסרטיביות הדיגיטלית של האיחוד מול אזורים אחרים בעולם. כדי למנוע מצבים שבהם עימותים במרחב הסייבר ייצאו מכלל שליטה, גיבש האיחוד האירופי באוקטובר 2017 את מה שכונה "ארגז כלים לדיפלומטיית סייבר", המגדיר מהם אמצעי הנגד האפשריים שיגבו מחיר מהתוקפים במקרה של מתקפת סייבר חיצונית. מסגרת הפעולה המתוכננת כוללת זימון דיפלומטים וסנקציות מדיניות, כלכליות ופליליות נוספות, לצד תגובות דיגיטליות. עם זאת, הבעיה הבסיסית – ייחוס המתקפה – קיימת גם בעולם של דיפלומטיית הסייבר. בנוסף לכך, השימוש ב"ארגז הכלים" אינו נתון להחלטה וולונטרית, אלא תלוי בתמיכתן פה אחד של כל המדינות החברות באיחוד. כל אלה מצטברים לכדי מכשולים המקשים על יצירת הרתעה הגנתית יעילה בסייבר.

מילות מפתח: סייבר, האיחוד האירופי, אסטרטגיה, הרתעה

מבוא

מאז שנודע דבר מתקפות הסייבר נגד רשתות מחשבים ומשרדי ביטחון והגנה של ממשלות אירופיות, מתעקשים קובעי מדיניות הביטחון שעל המדינות החברות באיחוד האירופי לפתח יכולות הגנת סייבר ותגובות סייבר הולמות יותר. האיחוד ממשיך, עם זאת, לדגול באסטרטגיית ביטחון סייבר שתתבסס על חוסנן של תשתיות טכנולוגיית המידע והתקשורת ועל דיפלומטיית סייבר. זאת, כחלק ממדיניות

ד"ר אנגרט בנדייק היא סגנית ראש החטיבה לאירופה במכון הגרמני לענייני ביטחון ועניינים בין־לאומיים בברלין.

החוץ והביטחון המשותפת שלו ומשאיפתו למצב את עצמו ככוח החותר לשלום. באוקטובר 2017 אימץ האיחוד את תוכנית "התגובה הדיפלומטית המשותפת של האיחוד האירופי לפעילות סייבר זדונית", המתמקדת בכלים לא צבאיים שמטרתם לתרום ל"צמצום האיומים בתחום ביטחון הסייבר, מניעת עימותים והגברת היציבות ביחסים הבין־לאומיים".[1] התרחבות רשת התשתיות הביאה את האיחוד האירופי לדבוק במדיניות של דיפלומטיית סייבר צעד אחר צעד, המבוססת על העיקרון של בדיקת נאותות (Due diligence).

מתקפות סייבר (דוגמת זו ששוגרה נגד תשתיות המידע והתקשורת של הממשלה הפדרלית הגרמנית[2]), ריגול סייבר, גניבת קניין רוחני, פשעי סייבר או הפצת מידע כוזב, לא רק משתקים את התקשורת ופוגעים בביטחון הסייבר, אלא גם יכולים להיות חלק מלוחמה היברידית. "היברידי" בהקשר זה פירושו שימוש מכוון, סמוי או גלוי, שעושים שחקנים מדינתיים ולא מדינתיים באמצעים אזרחיים וצבאיים במשולב. אמצעים אלה כוללים, לצד מתקפות סייבר, קמפיינים של דיסאינפורמציה, ריגול, לחץ כלכלי, שימוש ב"שליחים" (proxy) ופעילויות חתרניות אחרות. השימוש בגז עצבים שנעשה בלונדון הביאה את ראשי הממשלות וראשי המדינות של האיחוד האירופי להכריז, בסוף מארס 2018, על עמידה חד־משמעית לצד בריטניה, תוך איום על רוסיה שתישא באחריות. במסגרת זו נשקלו סנקציות נוספות, כמו גם פעולת תגמול בסייבר (hackback).[3]

הן האיחוד האירופי והן נאט"ו מיקדו את האסטרטגיות שלהם באירופה בהרתעה מבוססת חוסן, אם כי כל ארגון פנה לתחומים אסטרטגיים שונים. חלק ממעצמות הסייבר החלו לבנות את יכולות הסייבר ההתקפיות וההגנתיות שלהן, בעוד שהאיחוד האירופי ונאט"ו דוחפים את המדינות החברות לבנות יכולת הגנה משותפת. עם זאת, רק מספר קטן של מדינות באיחוד האירופי ובנאט"ו, וביניהן בריטניה, צרפת, אסטוניה והולנד, הן בעלות יכולות טכניות ותשתית משפטית להציב יכולות סייבר התקפיות.

1 "Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities", 13007/17 LIMITE, *Council of the European Union*, Brussels, October 9, 2017, p. 2.

2 Thorsten Severin and Andrea Shalal, "German Government under Cyber Attack Shores up Defenses", *Reuters*, March 1, 2018.

3 "Conclusions on the Salisbury Attack", *European Council*, March 22, 2018, http://www.consilium.europa.eu/en/press/press-releases/2018/03/22/european-council-conclusions-on-the-salisbury-attack/pdf.

הגנת סייבר: מגננה או מתקפה?

השאלה אם על מדינות מותקפות לנקוט אמצעי נגד התקפיים, דוגמת פעולת תגמול בסייבר, כדי לנטרל את מקור מתקפת הסייבר, היא נושא פוליטי ושנוי במחלוקת. אסטרטגיית אבטחת הסייבר של גרמניה מ־2016[4] קוראת לביטחון סייבר הגנתי ולהקמת כוח תגובה מהירה נייד במסגרת המשרד הפדרלי לביטחון המידע (BSI), וכן להקמת צוותים דומים בתוך המשטרה הפדרלית ובסוכנות מודיעין הפנים, שיהיו מסוגלים להגיב לאיומי סייבר על מוסדות ממשלתיים ותשתיות קריטיות. ממשלת הקואליציה החדשה בגרמניה אימצה את העמדה שלפיה גרמניה זקוקה לאמצעי סייבר צבאיים ואסטרטגיים, וכן לבסיס משפטי לפריסתם, כדי להגיב על התקפות סייבר, כמו אלו שהיו על הפרלמנט הפדרלי בשנת 2015 או על רשת התקשורת הממשלתית בשנת 2018.[5]

נאט"ו רואה במתקפות המתרחשות במרחב הסייבר צורה של לוחמה, המצדיקה את הפעלת פסקת ההגנה ההדדית של סעיף 5 באמנה הצפון אטלנטית. נאט"ו דן בימים אלה בשאלה האם התכנון המבצעי של הארגון צריך לכלול מרכיב של פעולות התקפיות ברשתות מחשבים מצד המדינות החברות. מאז פסגת נאט"ו בוורשה ב־2016, התחזק שיתוף הפעולה בין הארגון ובין האיחוד האירופי, והוא כולל חילופי מידע ותרגילי ביטחון סייבר משותפים.

נייר עמדה של משרד ההגנה הגרמני משנת 2016, העוסק במדיניות הביטחון הגרמנית ובעתיד הבונדסוור, מצביע על הקמת יחידה ארגונית שישית במספר בצבא גרמניה – יחידת מרחב הסייבר והמידע – המונה כיום כ־13,500 איש.[6] הקמת היחידה תאפשר שימוש ביכולות סייבר הגנתיות והתקפיות גם יחד, במקרה של צורך בהגנה עצמית או בהגנה הדדית במסגרת נאט"ו. השאלה אם יכולות התקפיות נכונות גם לזמן שלום עדיין שנויה במחלוקת. המבקרים טוענים כי התפשטות של תוכנות זדוניות לכדי מתקפת סייבר אינה מצדיקה את היתרונות ההרתעתיים קצרי הטווח שיכולות התקפיות אלו מציעות. הם עומדים על כך שנושאים הנוגעים לבניית אמון, לאמצעים להגברת הביטחון ולבקרת נשק צריכים להיות מטופלים על ידי האו"ם ו"הארגון לביטחון ושיתוף פעולה באירופה" (OSCE), וכי כל פיתוח של יכולות ביטחון סייבר התקפיות יוצר סיכון של הגברת חוסר האמון, חוסר ביטחון הדדי וסיכוי לעימותים. לשיטתם, רק דיפלומטיית סייבר ארוכת טווח,

4 "Building and Community, German National Cyber Security Strategy", *Federal Ministry of the Interior*, 2016, http://www.bmi.bund.de/cybersicherheitsstrategie/.

5 Melissa Eddy, "Germany Says Hackers Infiltrated Main Government Network", *The New York Times*, March 1, 2018.

6 "White Paper on German Security Policy and the Future of the Bundeswehr", *The German Federal Government*, 2016, https://bit.ly/2zXvJuE.

המתואמת ברמת האיחוד האירופי, תוכל לסייע בהשגת ביטחון לאירופה ולמנוע הסלמת סכסוכים.[7] אין ספק שלאיחוד האירופי יש אינטרס למצב את עצמו כמכתיב הנורמות בתחום ביטחון הסייבר באירופה ולהדגיש את חשיבותם של צעדים בוני אמון וביטחון בדיפלומטיית הסייבר הבין־לאומית.

סוגים שונים של דיפלומטיית סייבר

דיפלומטיית סייבר, בניגוד להגנת סייבר כוללת, מציעה אפשרות למנוע הסלמה של עימותים, ובכך היא מחזקת את הסיכוי לשלום. נציבים המופקדים על מדיניות חוץ בתחום הסייבר פועלים כיום ביותר משלושים מדינות. דנמרק אף מינתה שגריר לדיפלומטיית סייבר. דיפלומטיית סייבר במובנה הרחב ביותר כוללת אמצעי בניית אמון, וכן היבטים מסוימים של בניית נורמות בין־לאומיות, הגנה על נתונים, חופש ביטוי, ממשל באינטרנט והעמדה לדין, מכוח הסכמים בין־לאומיים, בגין אי־מתן סיוע משפטי הדדי. עם זאת, לממשלות רבות אין את הידע או את המשאבים הדרושים כדי לשמור על סטנדרטים בסיסיים של ביטחון סייבר, או אפילו כדי לזהות מתקפה המתבצעת דרך שרתים הנמצאים בשטחן. למרות זאת, רוב המדינות מביעות הסתייגות רבה מהרעיון להקים גוף רגולטורי מרכזי וכולל לאבטחת מרחב הסייבר מחשש לריבונותן הלאומית, ולכן מסמנות אותו כדבר בלתי מציאותי בשלב זה. סביר יותר להניח שמרחב הסייבר ומרחב המידע יוכפפו בהדרגה לריבונות הלאומית.[8] כך או כך, הרגולציה הממשלתית תפגר תמיד אחרי ההתפתחות הטכנולוגית של המגזר הפרטי. שותפויות ציבוריות־פרטיות מסתמנות, אפוא, כצורת הפיקוח הבולטת ביותר בתחום ביטחון הסייבר.

במישור המולטילטרלי, קבוצה של 25 מומחי ממשל בין־לאומיים, שכונסה על ידי העצרת הכללית של האו"ם בשנת 2015, הגיעה להסכמה כי יש ליישם את המשפט הבין־לאומי, לרבות את הזכות להגנה עצמית, גם על מרחב הסייבר.[9] עם זאת, הקבוצה לא הצליחה להגיע בקיץ 2017 להסכמה אם להקים מעין "מועצת ייחוס" (attribution council). תנאי מוקדם לקביעת ייחוס (שהוא הזיהוי הטכני, המשפטי והפוליטי של מבַצע מתקפת הסייבר) הוא יצירת שיתוף במידע רגיש בין

7 André Barrinha and Thomas Renard, "Cyber-Diplomacy: The Making of an International Society in the Digital Age", *Global Affairs* 3, no. 4-5 (2017): 353-364; André Barrinha, "Virtual Neighbors: Russia and the EU in Cyberspace", *Insight Turkey* 20, no. 3 (2018): 29-41.

8 Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, (Polity, Cambridge, UK, Malden, MA., 2017).

9 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", *United Nations General Assembly*, A/70/174, July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

צוותי CERT (צוותי תגובה לאירועי חירום במחשבים) ובין השירותים החשאיים וסוכנויות הביטחון.

המסגרות המולטילטרליות הבלתי יעילות הביאו לכך שהנשיאים שִי ג'ינפינג וולדימיר פוטין חתמו ב־2016 על הצהרה בילטרלית משותפת בשנחאי, שהכריזה על שלב חדש בשותפות האסטרטגית הכוללת בין סין ובין רוסיה. בייג'ין ומוסקבה הביעו דאגה מהשימוש לרעה שנעשה בטכנולוגיות מידע ותקשורת לצורך התערבות בעניינים פנימיים של מדינות, וקראו לקהילה הבין־לאומית לשתף פעולה על בסיס של כבוד ותועלת הדדיים ושיקולי צדק, ולספק מענה משותף לאיומים על אבטחת המידע.[10] ארצות הברית מסתמכת גם היא על הסכמים בילטרליים כדי להילחם בפשעי סייבר, כמו ההסכם בעניין זה שחתמה עם סין.[11]

מאז כישלון השיחות המולטילטרליות שנערכו בחסות האו"ם ב־2017, קוראים מומחי ביטחון סייבר להקמת "קואליציה של המוכנים" מקרב מדינות ה־G20 או ה־G7, כדי לקדם גיבוש של נורמות בין־לאומיות בתחום הסייבר. מסגרות דו־מסלוליות כמו "הנציבות העולמית ליציבות מרחב הסייבר", הן המובילות כיום בתחום זה.

חיזוק יכולת הייחוס נוגע לא רק למדינות, אלא גם למגזר הפרטי. בפברואר 2017 קראה חברת "מייקרוסופט" לכינון "אמנת ז'נבה הדיגיטלית",[12] והיוזמה האחרונה בנושא זה היא "אמנת האֶמון" שהשיקה חברת "סימנס" בכנס האבטחה במינכן בפברואר 2018,[13] העוסקת ברעיונות דומים. הפורום הכלכלי העולמי מבקש להקים "מרכז עולמי לביטחון הסייבר" כדי להיאבק בפשיעה בסייבר, וחותר גם הוא לשיפור שיתוף הפעולה בין המגזר הפרטי ובין רשויות המדינה, במה שמכונה "שותפויות ציבוריות־פרטיות".

10 "China, Russia Sign Joint Statement on Strengthening Global Strategic Stability", *Xinhuanet*, June 26, 2016, http://www.xinhuanet.com/english/2016-06/26/c_135466187.htm.

11 Adam Greer and Nathan Montierth, "How Are US-China Cyber Relations Progressing?", *The Diplomat*, November 1, 2017, https://thediplomat.com/2017/11/how-are-us-china-cyber-relations-progressing/.

12 Brad Smith, "The Need for a Digital Geneva Convention", *Microsoft*, February 14, 2014, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

13 "Charter of Trust Time for Action: Building a Consensus for Cybersecurity", *Siemens*, May 17, 2018, https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html.

מדיניות ביטחון הסייבר ומדיניות החוץ בסייבר של האיחוד האירופי

ביטחון סייבר הוא בעיה לא רק עבור מדינות, אלא גם עבור האיחוד האירופי כארגון. הבעיה חורגת מעֵבר לשאלה של חוסן הרשתות, של השוק הדיגיטלי או של העמדה לדין של פושעי סייבר, ונוגעת גם למדיניות החוץ והביטחון המשותפת של האיחוד האירופי ולמדיניות ההגנה והביטחון המשותפת שלו (ראו טבלה 1 להלן). שורה של גורמים כבר מתמודדים עם סוגיות מדיניות החוץ וביטחון הסייבר של האיחוד האירופי: "התגובה המשולבת למשברים פוליטיים" (IPCR) של האיחוד, ובעיקר "הסוכנות האירופית לאבטחת רשתות ומידע" (ENISA), "המרכז האירופי לפשעי סייבר" (EC3) ביורופול, "מרכז המודיעין וחדר המצב של האיחוד האירופי" (INTCEN), "מינהלת המודיעין של הצוות הצבאי של האיחוד האירופי" (EUMS INT) וחדר המצב שלה (EU SITROOM), יחידת INTCEN של האיחוד לניתוח איומים היברידיים (הידועה בשם Hybrid Fusion Cell), "צוות התגובה לאירועי חירום במחשבים של מוסדות וסוכנויות האיחוד האירופי" (CERT-EU), וכן "מרכז תיאום המענה בחירום של הנציבות האירופית" (ERCC). יש לציין גם גופים ומנגנונים חדשים שהוקמו על פי "ההנחיה לביטחון רשתות ומידע" (NIS), כגון "רשת צוותי IT בחירום של המדינות החברות" (CSIRT).

טבלה 1. ביטחון סייבר באיחוד האירופי: תחומי אחריות

CFSP: דיפלומטיית סייבר	**CSDP: הגנת סייבר**	**שוק אחיד**	**חופש, ביטחון, משפט**	
EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM EU Hybrid Fusion Cell ERCC	EDA GSA	ENISA רשת CSIRT CERT-EU	יורופול (EC3) Eurojust EU-LISA	האיחוד האירופי
משרדי חוץ	גופי הגנה, צבא וביטחון	רשויות המופקדות על NIS, צוותי CSIRT לאומיים	רשויות ניהול והגנה על נתונים	**רמת המדינה**

קיצורים: EDA: "סוכנות ההגנה האירופית"; EEAS: "שירות פעילות החוץ האירופית"; EU-LISA: "הסוכנות האירופית לניהול מערכות IT רחבות היקף בתחום החופש, הביטחון והמשפט"; GSA: "הסוכנות האירופית למערכות ניווט לווייני גלובליות"; SIAC: יכולת יחידנית לניתוח מודיעין.

האיחוד האירופי הקים בשנת 2015 את "קבוצת העבודה האופקית לנושאי סייבר", במטרה לתאם את ההיבטים הפוליטיים של מרחב הסייבר. הקבוצה נוטלת חלק הן בפעילויות חקיקה והן בפעילויות שאינן קשורות לחקיקה. יתרה מכך, המדינות החברות החליטו בפברואר 2015 לחזק את דיפלומטיית הסייבר ברמת האיחוד כחלק ממדיניות החוץ שלו. המהלך אושר בנובמבר 2016 במסגרת "התוכנית ליישום ביטחון והגנה".[14] גופים מרכזיים המתאמים את הניתוח האסטרטגי עבור מדיניות החוץ והביטחון המשותפת הם: צוות דיפלומטיית הסייבר ב"שירות פעילות החוץ האירופית"; יחידת INTCEN, המופקדת על המודִיעִין למצב בפן האזרחי; "מינהלת המודיעין של הצוות הצבאי של האיחוד האירופי", העושה זאת בפן הצבאי. כדי להרתיע מפני מתקפות סייבר ולהשתקם בעקבותיהן, וכדי לזהות את העבריינים, תלויים מומחי מחשב פורנזיים במקורות רבים הפועלים בכל הרמות הפוליטיות במדינות ובארגונים השונים. האיחוד האירופי מסתמך על שיתוף הפעולה הטוב השורר בין משרדי הממשלה ובין גופי הביטחון כדי ליצור תיאום בתחום זה.

חוקים מיוחדים חלים על המאבק בטרור. עם זאת, טרם גובשה מדיניות מתואמת של האיחוד האירופי, המחברת בין החובה להחליף מידע ובין המעקב והשימוש במידע משותף זה, שתהיה מגובה בהסכמים, אם כי מדיניות כזו נמצאת בבחינה מחודשת. ההגנה על השוק הדיגיטלי הפנימי במדינות האיחוד מצדיקה את הגברַת היכולות של הנציבות האירופית בעניין זה. הנציב לביטחון של האיחוד, ג'וליאן קינג, מופקד על נושא זה וכבר השיק חבילת חקיקה מרחיקת לכת לחיזוק החוסן הפנימי.

נייר עמדה משותף של האיחוד האירופי, מספטמבר 2017, שכותרתו "חוסן, הרתעה והגנה: בניית ביטחון סייבר חזק עבור האיחוד האירופי", מציע נקודות מוצא לשיתופי פעולה בבניית אמון וביטחון. אלו מתבססות על ארבעת יסודות ביטחון הסייבר של האיחוד האירופי.[15] "קבוצת העבודה האופקית לסוגיות הסייבר", שהיושב ראש שלה מתחלף ברוטציה, וכן "הוועדה לביטחון ופוליטיקה" (PSC), אחראיות על אמצעי יישום הולמים. יש לזכור כי מבחינה משפטית, המדינות החברות באיחוד האירופי חופשיות להשיק יוזמות משלהן.

14 "Implementation Plan on Security and Defence, Factsheet", *European External Action Service*, 2016, https://eeas.europa.eu/headquarters/headquarters-homepage/34215/implementation-plan-security-and-defence-factsheet_en.

15 "Resilience, Deterrence and Defence: Building Strong Cybersecurity in Europe", *European Commission*, 2017, https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe.

ארבעת יסודות ביטחון הסייבר של האיחוד האירופי הם:

- **היסוד הראשון**: ההנחיה בנושא מתקפות על מערכות מידע, משנת 2013,[16] לרבות הקנסות בגין מתקפות כאלו. הנחיה זו חלה על מקרים של שחקנים פליליים שאין להם קשר משמעותי עם מדינה נותנת חסות. כדי להתמודד עם האיום ההולך וגובר של פשעי סייבר חוצי גבולות, מתוכננים כלים חדשים, שניתן יהיה להפעילם לצורך העמדה לדין בצורה יעילה יותר. ההנחיה לגבי "ר•יות אלקטרוניות" ("e-evidence") נמצאת בשלב זה בדיונים, כשהמטרה היא לאפשר נגישות חוצה גבולות לראיות כאלו.[17] הנחיה נוספת שנמצאת בדיון עוסקת במאבק בהונאה ובזיוף בסביבה נעדרת מזומנים, דוגמת מטבע ה"ביטקוין". המטרה במקרה זה היא לשפר את שיתוף הפעולה בין הרשויות השונות של המשפט הפלילי.
- **היסוד השני**: שדרוג "הסוכנות האירופית לאבטחת רשתות ומידע" על ידי הגדלת צוות העובדים משמונים ל־125 איש והגדלת התקציב השנתי מ־11 ל־23 מיליון אירו. הסוכנות אמורה לארגן תרגילי ביטחון סייבר שנתיים כלל־אירופיים ולעודד שיתופי פעולה בין צוותי IT בחירום של המדינות החברות (CSIRT). בעבר הורחבו תרגילים אלה מדי פעם גם לבעלות ברית שאינן חברות. "הסוכנות האירופית לאבטחת רשתות ומידע" נועדה בעיקר ללוות את הקמתה ויישומה של מסגרת הסמכה כלל־אירופית. המטרה היא להפוך מוצרים ושירותים של טכנולוגיות מידע למאובטחים יותר באמצעות מתן תמריצים לשוק, ולאפשר למשתמשים לקבל החלטות מושכלות בבואם לרכוש מוצרים ושירותים כאלה. מערכות הסמכה שונות יעברו האחדה כדי לחזק את השוק הדיגיטלי האחיד למוצרים אמינים. צעדים אלה מבוססים על "ההנחיה לביטחון רשתות ומידע",[18] שאמורה הייתה להיכנס לתוקפה במאי 2018 ולשמש כאמת מידה להשגת שיפורים דומים גם ב"ארגון לביטחון ושיתוף פעולה באירופה"(OSCE).

16 "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision", *European Parliament*, 2005/222/JHA, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

17 "E-evidence – Cross-Border Access to Electronic Evidence", *European Commission*, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

18 "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union", *European Parliament*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

- **היסוד השלישי**: "שיתוף הפעולה המובנה והקבוע" (PESCO) שהוקם בדצמבר 2017 על ידי 25 שרי ההגנה של האיחוד האירופי.[19] נכון לנובמבר 2018, שבעה מתוך 34 פרויקטים של הגוף החדש מיועדים ספציפית לביטחון סייבר באירופה. על פי הדיווחים, פרויקטים אחרים שלו עוסקים בסטנדרטיזציה של מערכות לחיילים – ציוד אלקטרוני, תקשורת שפה ונתונים ותוכנה. יוון מתכננת לפתח צוות חירום אירופי לענייני טכנולוגיות מידע, וליטא מבקשת להיות אחראית על הקמת מערכת הגנת סייבר אירופית. הרעיון הוא ליצור מעֵין "אזור שנגן בסייבר", שיילחם בפשיעה באינטרנט ויפעל באופן שיחצה את הגבולות הלאומיים. הבנק האירופי להשקעות מתכוון להשקיע עד סוף 2020 יותר משישה מיליארד אירו בפיתוח מה שמכונה "טכנולוגיות כפולות שימוש", שנועדות לביטחון סייבר צבאי ואזרחי.
- **היסוד הרביעי**: ניהול דיאלוגים בילטרליים בנושא הסייבר בין האיחוד האירופי ובין גורמים חיצוניים, במסגרת הסכמי השותפות האסטרטגית שלו עם ארצות הברית, קנדה, סין, דרום קוריאה ומדינות נוספות. האיחוד גם מציע לנסח אסטרטגיה לשיתוף פעולה בין־לאומי במרחב הסייבר ולמניעת עימותים, באופן שיהיה תואם את רפורמת ביטחון הסייבר של ספטמבר 2017. כצעד ראשון, עדכן האיחוד את אמצעי דיפלומטיית הסייבר ושל הגנת הסייבר שלו, וכן את הנחיותיו בעניין הפיקוח על ייצוא סחורות בעלות שימוש כפול.

תגובה דיפלומטית משותפת לפעילות סייבר זדונית

העלייה במספר מתקפות הסייבר אילצה את השחקנים הבין־לאומיים השונים לשקול כיצד להגיב עליהן כראוי. ממשל אובמה הטיל ב־2014, לראשונה, סנקציות חד־צדדיות על צפון קוריאה, לאחר שחברה בת אמריקאית של תאגיד "סוני" נפלה קורבן למתקפת סייבר קטלנית, שבמהלכה הועתקו כל המידע והנתונים שלה.[20] שנתיים לאחר מכן חזרה ארצות הברית להטיל סנקציות לאחר שנתוני כוח האדם של הממשל האמריקאי "נשאבו", כחלק ממתקפת סייבר רחבת היקף. בעקבות ההתערבות הרוסית לכאורה במסע הבחירות לנשיאות ארצות הברית ב־2016,

19 "Permanent Structured Cooperation (PESCO) – Factsheet", *European External Action Service*, 2018, https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en.

20 David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea after Sony Case", *The New York Times*, January 2, 2015, https://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html.

הטיל הממשל האמריקאי, במארס 2018, סנקציות על חמישה ארגונים וחברות ו־19 חשודים, בנימוק של "פעולות סייבר זדוניות" מצידה של רוסיה.[21]

האיחוד האירופי דן לראשונה בפברואר 2015 בצורך בדיפלומטיית סייבר משותפת. ביוני 2017 הציע האיחוד לבנות "ארגז כלים לדיפלומטיית סייבר", כדי לספק מענה דיפלומטי משותף לפעולות סייבר זדוניות.[22] מטרתו העיקרית של "ארגז הכלים" הייתה להבטיח יכולת תגובה למדיניות החוץ והביטחון של האיחוד, שתהיה מתחת לסף של עימות מזוין. יכולת כזו נועדה להשלים את צעדי האיחוד מכוח "ההנחיה לביטחון הרשתות והמידע", על ידי דרישה לתקינת סף וחובת דיווח, וכן לבניית מערכות של טכנולוגיות מידע ותקשורת עמידות עבור "השוק הדיגיטלי האחיד". דיפלומטיית סייבר כזו ברמת האיחוד האירופי תאפשר להפעיל אמצעים פוליטיים, לרבות אמצעים מגבילים, במסגרת מדיניות החוץ והביטחון המשותפת, כתגובה על מתקפות סייבר.

באוקטובר 2017 אומץ "ארגז הכלים" המתוכנן לדיפלומטיית הסייבר תחת השם החדש: "טיוטה לקווים מנחים למסגרת לתגובה דיפלומטית משותפת של האיחוד האירופי נגד פעולות סייבר זדוניות". "הארגז" נועד לסייע למדינות האיחוד לשתף פעולה בבלימת איומים מיידיים וארוכי טווח ולהרתיע עבריינים ותוקפים פוטנציאליים בטווח הארוך. נראה שלכל אחת ממדינות האיחוד בנפרד לא הייתה יכולת מספקת להשפיע על חישובי עלות־תועלת של התוקפים; לעומת זאת, דיפלומטיית הסייבר של האיחוד האירופי הציעה ערך מוסף אסטרטגי, בשל יכולתה להטיל סנקציות, או לחילופין להציע תמריצים חיוביים.

האיחוד האירופי התחייב לפעול על פי העקרונות הבין־לאומיים, תוך שמירה על בדיקת נאותות במרחב הסייבר. בכוונתו גם לחזק את דיפלומטיית הסייבר שלו על ידי חילופי מידע עם צדדים שלישיים, כחלק מהמאבק במתקפות סייבר. צוות מומחי הממשל של האו"ם אימץ גם הוא את עקרון בדיקת הנאותות בדוח הסופי שלו, אותו הגיש ביוני 2015.[23] על פי דוח זה, מדינות אחראיות לוודא כי שטחן הריבוני ומערכות המחשוב והתשתית הממוקמות בו, או נמצאות בשליטת

21 "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks", *US Department of the Treasury*, March 15, 2018, https://home.treasury.gov/news/press-releases/sm0312.

22 "Draft Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox) 9916/17", *European Council*, June 7, 2017, http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

23 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", *United Nations*, July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

אותן מדינות בצורה אחרת כלשהי, אינם מנוצלים למתקפות על תשתיות של מדינות אחרות.

חמשת האמצעים של "ארגז הכלים"

האיחוד האירופי מסתמך בדיפלומטיית הסייבר שלו על "ארגז הכלים" של מדיניות החוץ והביטחון המשותפת. ניתן לחלק את כלי העבודה של "הארגז" לחמש קטגוריות: אמצעים מניעתיים; אמצעים שיתופיים; אמצעים מייצבים; אמצעים מגבילים; אמצעים לתגובות של הגנה עצמית מכוח החוק של כל אחת מהמדינות החברות. את האמצעים המדיניים קובעת מועצת האיחוד האירופי, בסיוע "שירות פעילות החוץ האירופית". במקרים חמורים, פעילויות סייבר זדוניות יכולות להביא לנקיטת אמצעי ענישה ולשימוש בכוח או אף בהתקפה חמושה, בהתאם לחוק הבין־לאומי ולמגילת האומות המאוחדות. במקרים כאלה, המדינה החברה מקבלת החלטה ריבונית להפעיל הגנה עצמית עצמאית, או קולקטיבית מכוח סעיף 51 של מגילת האו"ם, ובהתאם לדין הבין־לאומי וההומניטרי.

אמצעים מניעתיים

האיחוד האירופי מנהל דו־שיח בנושא הסייבר במסגרת דיאלוגים מדיניים עם מדינות שלישיות, שמטרתם להשפיע על ההתנהגות ועל העמדה של שותפיו לשיח. האיחוד גם תומך בצעדים בוני אמון, כמו אלה שפותחו על ידי "הארגון לביטחון ושיתוף פעולה באירופה". דיאלוגים עם ארגונים אזוריים, כגון האיחוד האפריקאי או ASEAN (איחוד מדינות דרום־מזרח אסיה), חשובים במיוחד. בדרך זו יכולים האיחוד האירופי והגוף האזורי שניצב מולו להגדיר כיצד ניתן לשכלל את יכולות האזור להשתמש במרחב הסייבר (המכונות "בניית יכולת סייבר"). זאת, באמצעות הסכמי התאגדות (אסוציאציה), הסכמי שותפות וכן שיתופי פעולה, או באמצעות "המכשיר ליציבות ולשלום" (IcSP).

אמצעים שיתופיים

כדי להקל על הטיפול בתקרית מתמשכת, המשלחת של האיחוד האירופי במדינה המארחת יכולה להעביר איגרת דיפלומטית (Demarche) לממשלה של אותה מדינה. מהלך כזה מחייב הוראה מהנציב העליון של האיחוד לענייני מדיניות חוץ וביטחון. במצב של עימות, ראש משלחת האיחוד יכול להעביר הצעה לערוך שיחות מקיפות, או להסתפק בהעברת מסרים בנושאי מפתח. האיגרת הדיפלומטית יכולה להתנסח ולהישלח גם בעזרת מדינה שלישית. סוג כזה של פתרון אינו אפשרי במקרים שבהם ראש המשלחת של האיחוד האירופי נקרא לחזור לארצו בשל מצב של עימות.

אמצעים מייצבים

אמצעים מסוג זה ממלאים תפקיד של מסר, בהיותם איתות אסטרטגי לתוקף הפוטנציאלי שעליו להימנע מלעסוק בפעילות סייבר זדונית. מועצת אירופה יכולה לקבוע פעולה או עמדה של האיחוד האירופי, אולם רק אם אלו התקבלו פה אחד. היא גם יכולה להעביר החלטה לממש פעולה כזו. במקרה כזה תידרש הצבעה ברוב קולות, למעט כשמדובר בפעולות הנוגעות לצבא או להגנה (סעיף 31, פסקה 2 באמנת האיחוד האירופי). הנציב העליון של האיחוד לענייני מדיניות חוץ וביטחון יכול גם למסור הצהרה "בשם האיחוד האירופי", אם כי תידרש לכך הסכמה מראש של כל מדינות האיחוד. הסכמה כזו תתקבל בדרך כלל, אלא אם יש צורך בתגובה מיידית, או אם האיחוד האירופי צריך תחילה לגבש את עמדתו לנוכח מצב חדש, או אם שונתה עמדה קיימת. במקרים שנדרשת תגובה מהירה, אך לא ניתן להגיע להסכמה בקרב 27 המדינות החברות, הנציב העליון יכול לפרסם את ההצהרה על אחריותו האישית.

סנקציות

האיחוד האירופי רשאי להטיל אמצעים מגבילים (סנקציות) בניסיון לקדם מטרות מדיניות בעקבות מתקפות סייבר חמורות. צעדים כאלה יהיו, בדרך כלל, מכוונים כלפי גורמים רשמיים של מדינות שלישיות, אך גם כלפי חברות ממשלתיות, ישויות משפטיות או אישיות טבעית אחרת. על מועצת אירופה להצביע פה אחד על הטלת הסנקציות, והן יהיו חייבות לעלות בקנה אחד עם מטרות מדיניות החוץ והביטחון המשותפת, לפי סעיף 24 של אמנת האיחוד האירופי.

ניתן לחלק את הסנקציות לשתי קטגוריות עיקריות: כאלו שנקבעות באופן עצמאי על ידי האיחוד האירופי, וכאלו שהאיחוד האירופי מחויב להטיל בעקבות החלטה של מועצת הביטחון של האו"ם. על פי חוקי האיחוד, סנקציות חייבות להיות ממוקדות. לדוגמה, ניתן להכניס חברות או אנשים מסוימים לרשימת הסנקציות כדי לחסום חשבונות בנק שלהם, כל עוד נשמרים כללי סף שקובע החוק. תנאים מוקדמים נוסחו כדי לשמור על החוקיות של מקרים כאלה, למשל, הקביעה כי המיועדים לסנקציות צריכים לקבל הסבר על הסיבות להכללתם ברשימה והזדמנות להגיש ערר.

תמיכה בתגובה חוקית של מדינה חברה

אמנת ליסבון כוללת סעיפי סולידריות וסיוע הדדי, אותם ניתן להפעיל בעקבות מתקפות סייבר חמורות. פסקת הסולידריות (סעיף 222 לאמנת התפקוד של האיחוד האירופי) קובעת כי המדינות החברות יעניקו תמיכה הדדית כאשר אחת או יותר מהן תיפול קורבן למתקפות טרור, לאסונות טבע או לאסונות מעשה ידי

אדם (כולל מתקפת סייבר חמורה). הנוהל ליישום סעיף זה באמנה הוגדר בהחלטה של מועצת אירופה מיולי 2014.

פְּסקת הסיוע ההדדי, המופיעה בסעיף 42 תת־סעיף 7 של אמנת האיחוד, מקבילה למדי לסעיף 5 באמנת נאט"ו, אם כי סעיף 5 נותן עדיפות לחברות נאט"ו. סעיף הסיוע ההדדי של האיחוד הופעל לראשונה על ידי צרפת בנובמבר 2015, בעקבות פיגועי הטרור בפריז. "התגובה הדיפלומטית המשותפת של האיחוד האירופי לפעולות סייבר זדוניות", מאוקטובר 2017, קובעת כי תגובות התואמות את הדין הבין־לאומי אינן מחייבות ייחוס חד־משמעי של מתקפת סייבר למקור או לתוקף ספציפיים. דבר זה עולה בקנה אחד עם הפרשנויות של מומחים למשפט בין־לאומי, המעוגנות ב"מדריך טאלין 2", בדבר החלת החוק הבין־לאומי על מרחב הסייבר.

פיקוח על הייצוא

האיחוד האירופי מתכוון לקדם את דיפלומטיית הסייבר שלו ואת שאיפתו לבדיקת נאותות באמצעות שליטה קפדנית יותר על ייצוא סחורות בעלות שימוש כפול. הנחיית השימוש הכפול, ממאי 2009, מסדירה את דרישות הרישוי המשותפות של המדינות החברות באיחוד האירופי במצבים של ייצוא, רכש והעברה של סחורות כאלו. באמצע דצמבר 2017 פרסמה הנציבות האירופית נוסח חדש לנספחים I, IIa עד IIg ו־IV של ההנחיה.[24] העדכון עסק בעיקר בפיקוח חדש על מוצרים מסוימים, כגון חומרות של טכנולוגיות מידע. הסחורות סווגו ככפופות לפיקוח (נספח I) על בסיס: (1) התנאים הקיימים באמנות ובהתחייבויות בין־לאומיות, ובמיוחד החלטת מועצת הביטחון של האו"ם 1540, אמנת הנשק הכימי ואמנת הנשק הביולוגי, וכן (2) רשימות פיקוח של משטרי ייצוא בין־לאומיים מולטילטרליים, ובראשם "הסדר ואסנאר", "קבוצת ספקיות הגרעין", "קבוצת אוסטרליה" ו"משטר הפיקוח על טכנולוגיית טילים" (MTCR). רשימות אלו מתעדכנות באופן תדיר. ייצוא סחורות ספציפיות למדינות הנתונות לסנקציות כפוף לא רק לפיקוח הדוק יותר; במקרים רבים יש לקבל אישור נפרד גם לייצוא סחורות בעלות שימוש כפול. אי־ציות לתנאים עלול לגרור עונשים או קנסות כבדים.

בדיקת נאותות – שלב אחר שלב

דרישת האיחוד האירופי להסכמה פה אחד מקשה על מיצובו ככוח משכין שלום. המדינות החברות מפגינות לא רק אמביוולנטיות אסטרטגית רבה (כמו, למשל,

24 "Commission Delegated Regulation (EU) 2017/2268 of 26 September 2017 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items", *Official Journal of the European Union* 60, December 15, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2017:334:FULL&from=EN.

במדיניותן כלפי רוסיה), אלא גם חוסר קוהרנטיות בפעולותיהן בענייני חוץ. שאיפת האיחוד האירופי לפעול ככוח משכין שלום מתבטאת ברצונן של המדינות החברות בו לחזק את עקרון בדיקת הנאותות באמצעות הכלים המדיניים שמציעה מדיניות החוץ והביטחון המשותפת.

בדיקת נאותות היא עיקרון מקובל היטב במשפט הבין־לאומי, המתבסס על הרעיון שהאיחוד האירופי לא רק חייב להבטיח שהכללים נשמרים בתחום השיפוט שלו, אלא גם לשאת באחריות לתוצאות מעשיו מחוץ לגבולותיו, למשל, באמצעות מדיניות ייצוא קפדנית יותר. כיום, יותר מתמיד, יש להחלטות האיחוד השלכות מעֵבר לתחום השיפוט שלו, ולכן עליו ליצור קוהרנטיות בתחום זה. כאשר הדבר נוגע למרחב הסייבר, לא די שהמדינות החברות יימנעו מהכרעות לא אחראיות הנעשות באופן עצמאי; חובתן היא גם ליטול על עצמן לפעול ביחד עם מדינות אחרות ולעשות כל מה שיתרום, בגבולות הסביר, ל"מרחב סייבר פתוח, כוללני, חופשי, שוחר שלום ובטוח".

השאלה עד כמה צריכות ממשלות המדינות החברות באיחוד האירופי להיערך לצעדי נגד טכנולוגיים, או אפילו לביצוע פעולות תגמול בסייבר, כפי שקורה כיום במקרה של רוסיה, נתונה לוויכוח. במידה שמדינה חברה תבחר להפעיל הגנה עצמית, כפי שהיא מוגדרת בסעיף 51 של מגילת האו"ם, ובהתאם למשפט הבין־לאומי ולמשפט ההומניטרי, הדבר יהיה בגדר מהלך מסלים ברמה הגבוהה ביותר של הסיוע ההדדי בקרב מדינות האיחוד האירופי. השלב הסופי של ניהול המשבר יהיה, לפיכך, עצירת המתקפה המתמשכת באמצעות הגנה אקטיבית, והמוצא האחרון יהיה פעולת תגמול בסייבר, כלומר פגיעה ממוקדת בשרת שממנו יצאה המתקפה. מהלך כזה יעמוד בעקרון בדיקת הנאותות רק אם המתקפה המתמשכת צפויה להסתיים בהשלכות חמורות שיאיימו על עצם קיומה של המדינה, ואם מוצו כל האמצעים האחרים. המסגרת המשפטית וחלוקת הסמכויות שפעולה כזו מחייבת לא הוגדרו עדיין, גם לא ברמה הלאומית.

הכלים החשובים והיעילים ביותר של האיחוד האירופי בהקשר זה הם מניעה וגילוי. המניעה כוללת את הצעדים הנכללים ב"הנחיה לביטחון רשתות ומידע", כגון אכיפה של תקינת סף ודרישות דיווח על מפעילי תשתיות קריטיות. ספקי תקשורת רשאים לנתח את תנועת הנתונים במקרה של שיבושים, ואם יש צורך, גם לחסום את העבריינים שזוהו.

חשיפה פירושה הבהרה וייחוס של המתקפה. גורם מכריע בהקשר זה היא ההערכה הפוליטית. עליה לקחת בחשבון את התמונה הכוללת של תקריות הסייבר ולחזות איומים היברידיים בעלי רלוונטיות צבאית. כאשר מדובר בהתקפות מקצועיות, נדרש שימוש בדיפלומטיית סייבר בין מדינות החולקות תפיסה דומה, כדי שגורמי הביטחון שלהן יחלקו מידע לצורך ניתוח חלקי הקוד ואופן התנהלותה של המתקפה.

ניתוחים מסוג זה מאפשרים להסיק מסקנות לגבי קבוצות ההאקרים ומקורן. "רשת צוותיIT בחירום של המדינות החברות" והיכולות הטכניות שלה נועדו לאפשר חילופי מידע דומים לצורך הגנה על תשתיות קריטיות. דיפלומטיית סייבר מחייבת החלפת מידע גם בין רשויות ועסקים. קבוצות CERT ציבוריות ופרטיות ושיתופי פעולה בתעשייה הכרחיים גם הם לאיגום ידע ומומחיות בדיפלומטיית סייבר.

דיפלומטיית סייבר היא מרכיב חשוב בביטחון הלאומי בסייבר. יחד עם זאת, עליה לשלב גם את הממד הכלל־אירופי ואפילו את הממד העולמי. אין די בחקירות שיתבססו אך ורק על מידע ברמה הלאומית. "מסגרת התגובה הדיפלומטית המשותפת של האיחוד האירופי לשנת 2017" מציעה מדיניות ביטחון סייבר שאינה צבאית. מדיניות כזו תסייע להתגבר על הדחף להגיב באופן מיידי על איומים במרחב הסייבר, ובמקום זאת נותנת עדיפות למהלכים מדיניים, כחלק ממדיניות החוץ והביטחון המשותפת של האיחוד, המבקש להטביע את חותמו ככוח משכין שלום. נכון יעשו שותפיו ויריביו של האיחוד ברחבי העולם כשיפרשו גישה זו שלו כמסר מדיני מובהק.