אסטרטגיית הסייבר של גרמניה – היערכות ממשלתית וצבאית מול איומי הסייבר

עמרי וקסלר

גרמניה היא מדינה מובילה באיחוד האירופי ואחת מהכלכלות החזקות בעולם. כתוצאה מכך היא מהווה מטרה מרכזית למתקפות קיברנטיות מצד מדינות, ארגוני טרור וארגוני פשע. התגברות האיום על הדמוקרטיה הגרמנית באמצעות קמפיינים של הפצת מידע כוזב, לצד האיום עליה מצד רוסיה, הובילו לשינוי בתפיסת הביטחון הגרמנית והביאו את ממשלת גרמניה לחתור להגברת עצמאותה בתחום הסייבר ולהתבססות על יכולות התקפיות במרחב זה. הבנת דרכי התמודדותה של גרמניה עם איומי הסייבר ותוכניותיה העתידיות בנושא זה חשובה לצורכי למידה והשוואה, וכן כדי לספק תובנות חדשות בסוגיה זו, במיוחד עבור מדינות דמוקרטיות אחרות.
בחלקו הראשון של המאמר מתוארים ההיערכות של ממשלת גרמניה בתחומי האבטחה הקיברנטית, שיתוף הפעולה בין הרשויות הגרמניות וכן היערכויות הקשורות בכוח אדם ובחיזוק המוסדות הרלוונטיים. בחלקו השני מתוארות ההיערכות ברמה הביטחונית־צבאית והדרך שבה מתאימה עצמה גרמניה לאתגרים החדשים. החלק האחרון במאמר בוחן את תמונת המצב בפן הבין־לאומי וכיצד רואה גרמניה את תפקידה כמובילה בתחום הסייבר בזירה הבין־לאומית.

מילות מפתח: אבטחה קיברנטית, גרמניה, אסטרטגיה, היערכות ממשלתית, היערכות צבאית.

רקע

ב־23 בפברואר 2011 פרסמה גרמניה אסטרטגיה מקיפה לתחום הסייבר. המסמך מגדיר את תפיסת האיום הקיברנטי, קובע קווים מנחים לאסטרטגיית אבטחה קיברנטית ומגדיר מטרות וצעדים ליישומם. הצעדים אותם נקטה גרמניה מאז

עמרי וקסלר הוא חוקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון ובמרכז למחקר סייבר בינתחומי ע"ש בלווטניק, אוניברסיטת תל אביב.

פרסום האסטרטגיה משנת 2011 עסקו בהגנה על תשתיות קריטיות, בהגברת מודעות האזרחים ובהטלת אחריות על יצרנים לספק מוצרים מאובטחים, בחיזוק אבטחת ה־IT בקרב הרשויות, בהקמת המרכז הלאומי להגנה קיברנטית (Cyber Abwehrzentrum – Cyber A-Z), בהקמת מועצה לאומית לאבטחה קיברנטית, בייעול המאבק בפשיעה במרחב הקיברנטי ובהתייצבות גרמניה כגורם מפתח בחזית המאמצים להגנת הסייבר באירופה וברחבי העולם.

בנובמבר 2016 אישר הקבינט הגרמני מסמך אסטרטגיה חדש בנושא אבטחת הסייבר, שפורסם מטעם משרד הפנים. האסטרטגיה החדשה הרחיבה את קודמתה מ־2011 ופורטו בה ארבעה תחומים מרכזיים שבהם על גרמניה לפעול: שימוש בטוח ועצמאי בסביבה הדיגיטלית; שיתוף פעולה בין המדינה והמערכת הכלכלית הגרמנית בתחום הסייבר; בניית מערך אבטחה קיברנטית יעיל בקרב המגזר הציבורי; הפיכת גרמניה לגורם מרכזי במדיניות הסייבר האירופית והעולמית.

תפיסת האיום

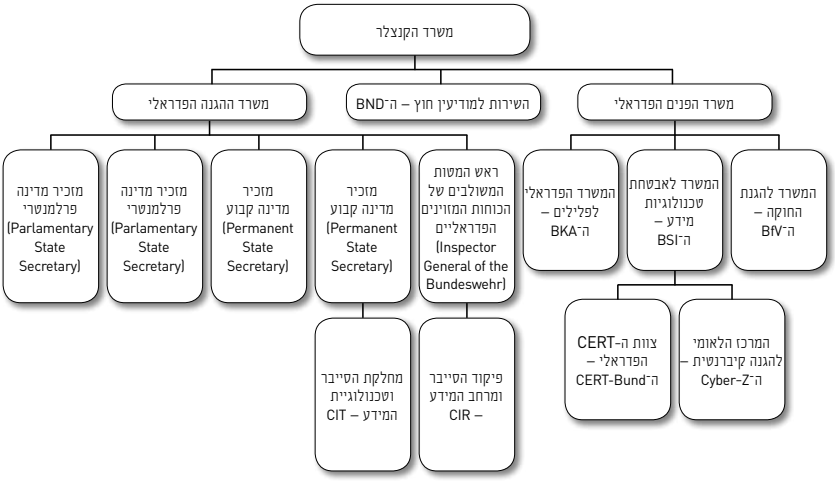
מסמך האסטרטגיה הגרמני משנת 2011 הציג את האיום הקיברנטי באופן כללי למדי ותיאר את מורכבות המתקפות הקיברנטיות. לעומתו, המסמך שפורסם בשנת 2016 הצביע על החשיבות הגוברת שמעניקה גרמניה לתחום הסייבר לאור העלייה במספר המתקפות הקיברנטיות ובמורכבותן. מסמך האסטרטגיה משנת 2016 עוסק, בין השאר, בנזק הנגרם ממתקפות קיברנטיות בתחומים החברתי, הכלכלי, הפוליטי והאישי, ומתאר אותן כאיום על היציבות, הסדר הציבורי והדמוקרטיה. המסמך מ־2016 גם מגדיר מטרות שפגיעה בהן תגרום לנזק ציבורי ופרטי רב. ביניהן:

- מתקפה על תשתיות קריטיות, ובמיוחד על תשתיות האנרגיה ורשת החשמל.
- מתקפה על תשתיות בנקאיות ומוסדות פיננסיים וביצוע מניפולציה על הבורסה.
- מניפולציה של מערכות אוטונומיות, השתלטות על תעבורת מידע הנשלטת על ידי מערכות IT, וכן מניפולציות על מערכות IT בתחום הבריאות.
- הפצה של מידע כוזב, דיווחים מטעים וחדשות מזויפות, המאפשרת לבצע מניפולציה של דעת הקהל, ועל כן מהווה סכנה לחברה החופשית ולדמוקרטיה.

משרד הפנים הגרמני, שהיה כאמור האחראי לניסוח האסטרטגיה, זיהה סוגים שונים של תוקפים ושל מניעים לביצוע מתקפות במרחב הקיברנטי: הרקע למתקפות הוא רחב ויכול להיות אידיאולוגי או פלילי. המבַצעים עלולים להיות ארגוני טרור, ארגוני פשע מאורגן, יחידות צבא או שירותי מודיעין של מדינות. הרקע המגוון של התוקפים ומקצועיותם מקשים על יכולות הגילוי והמעקב וכן על ניתוח המתקפות. מחברי המסמך מזהירים מפני עימותים פוליטיים או צבאיים שעלולים להיות מלווים

בעימות במרחב הקיברנטי. עימות במרחב זה עשוי להסלים למלחמת סייבר של ממש, או אפילו למתקפות סייבר שמתחת לסף של עימות מזוין.

תמונת מצב האיומים מורכבת ממספר רב של שחקנים בעלי יכולות ומניעים שונים. על כן, מחברי המסמך מסַכמים כי אמצעי ההגנה הקלאסיים על מערכות ה־IT הקיימות אינם מספיקים. הם מניחים כי מספר תקיפות הסייבר צפוי לעלות, כי מורכבותן תגבר וכי המטרות המרכזיות של התקפות הסייבר יהיו החברה הגרמנית, הכלכלה והתעשייה הגרמניות, וכן הדמוקרטיה הגרמנית.



תרשים: גופי הביטחון והסייבר בגרמניה

היערכות ממשלתית

גופי הממשל האחראים על תחום הסייבר בגרמניה הם: המשרד לאבטחת טכנולוגיית מידע (BSI), המשרד להגנת החוקה, המשמש כסוכנות ביטחון הפנים (BfV), שירות מודיעין החוץ (BND), המשרד הפדרלי לפלילים (BKA), משרד ההגנה (BMVg), משרד הפנים (BMI) והמשרד להגנת הציבור וסיוע למקרי אסון (BBK), המקביל לפיקוד העורף בישראל.

המשרד לאבטחת טכנולוגיית מידע

ה־BSI (Bundesamt für Sicherheit in der Informationstechnik) הוא משרד פדרלי הנמצא תחת סמכותו של משרד הפנים ומתפקד גם כרשות הלאומית לאבטחה קיברנטית. ה־BSI הוקם בשנת 1991 במטרה לספק שירותי IT לגופי ממשלה, ליצרני מערכות IT וכן לספקים ולמשתמשים. כיום אחראי ה־BSI להגנה על טכנולוגיית המידע של גרמניה ועל יישום מדיניות אבטחת המידע הלאומית. כן הוא אחראי

על מגוון פעילויות, כגון התרעה, מניעה ותגובה לתקריות, אזהרות מפני נקודות תורפה במוצרים ומפני תוכנות נוזקה, בניית ערוצי הדרכה והעלאת מודעות בקרב גופי ממשלה והציבור. כמו כן אחראי המשרד על חילופי מידע עם משרדי ממשלה, מוסדות וארגוני המגזר הפרטי, על ניסוח תקני אבטחה למפעילי תשתיות קריטיות ולמוצרים וכן על תהליכי הסמכה והכשרה של ארגונים ומוצרים.[1]

ה־BSI אחראי על גופים נוספים העוסקים בהתמודדות עם איומי סייבר, כגון המרכז הלאומי להגנה קיברנטית (Cyber A-Z) צוות ה־CERT הפדרלי (CERT-Bund) וה־CERT האזרחי (Bürger-CERT). הגוף האחרון אחראי על הגברת מודעות הציבור והעסקים הקטנים לאיומי סייבר.[2]

חיזוק המרכז הלאומי להגנה קיברנטית

Cyber A-Z הוא מוסד פדרלי להגנה מפני מתקפות אלקטרוניות על תשתיות ה־IT של גרמניה ועל המגזר הכלכלי שלה. המרכז הוקם על בסיס החלטת קבינט מפברואר 2011 והחל לפעול ביוני אותה שנה תחת המשרד לאבטחת טכנולוגיית מידע (BSI). Cyber A-Z ממוקם בעיר בון.[3]

המרכז הלאומי להגנה קיברנטית אינו מהווה ישות עצמאית והוא פועל יוצא של שורת הסכמי שיתוף פעולה בין הרשויות הגרמניות העוסקות בהגנה קיברנטית. על כן, ההפרדה בין תחומי השיפוט והאחריות של הרשויות השונות, ובעיקר בין המשטרה לשירותי המודיעין, נשמרת גם במהלך שיתוף הפעולה במסגרת המרכז.

המשימות המרכזיות של המרכז הלאומי להגנה קיברנטית הן מניעת מתקפות סייבר, אספקת מידע והתרעה מוקדמת על מתקפות כאלו. המרכז משתף מידע על הפרופילים והזהויות של השחקנים העומדים מאחורי מתקפות הסייבר, וכן משתף מידע סביב נקודות תורפה של מוצרי IT.

במסמך האסטרטגיה מ־2016 הומלץ כי Cyber A-Z ימשיך להתפתח כמרכז תיאום וכי תוקנה לו בעתיד יכולת ניתוח עצמאית ויכולת בניית תמונת מצב שתתאר במדויק את המתרחש. כמו כן הומלץ כי המרכז הלאומי להגנה קיברנטית יפעל גם כמרכז לאימונים ולתרגולים משותפים של צעדי התמודדות עם התקפות סייבר.[4]

---

1 Melissa Hathaway et al., "Germany: Cyber Readiness at a Glance", *Potomac Institute for Policy Studies*, October 2016, pp. 5-7, http://www.potomacinstitute.org/images/CRI/CRI_Germany_Profile_PIPS.pdf; "Cyber-Sicherheitsstrategie für Deutschland 2016", *Bundesministerium des Innern*, 2016, p. 17.

2 Hathaway et al., "Germany: Cyber Readiness at a Glance", pp. 5-7.

3 הרשויות הממלאות תפקיד מרכזי בתפעול המרכז הלאומי להגנה קיברנטית הן המשרד להגנת החוקה, המשרד לאבטחת טכנולוגיית מידע והמשרד להגנת הציבור וסיוע למקרי אסון. רשויות נוספות המעורבות במידע ושיתוף פעולה במסגרת פעילות המרכז הן המשרד הפדרלי לפלילים, שירות מודיעין החוץ הגרמני, המשטרה הפדרלית והצבא (הבונדסוור).

4 "Cyber-Sicherheitsstrategie für Deutschland 2016", p. 28

חיזוק יכולות הניתוח והתגובה של משרדי הממשלה

גרמניה משקיעה בהקמת צוותי תגובה ניידים (Mobile Incident Response Teams – MIRT), הכפופים למשרד לאבטחת טכנולוגיית מידע. מטרתם של צוותים אלה היא לנתח את המצב בזמן מתקפה ולסייע לצוותים המקומיים להתמודד עם האירוע והשלכותיו. הצוותים הניידים נועדו לתת מענה על פי בקשה, כדי לסייע לגופים חוקתיים, לרשויות פדרליות, למפעילי תשתיות קריטיות ולמתקנים חשובים. מטרת הסיוע היא בעיקר התמודדות עם האירוע, התאוששות וחזרה לשגרה.[5] צוותי התגובה הניידים אמורים לקבל סיוע מיחידות מיוחדות של המשרד הפדרלי לפלילים ומהמשרד להגנת החוקה.

צוותים נוספים אמורים לקום תחת המשרד הפדרלי לפלילים. צוותים אלה, שייקראו "כוחות לתגובה מהירה" (Quick Reaction Force), יהוו יחידה משפטית שתפקידה יהיה לאפשר תגובה מהירה למתקפות סייבר באמצעות תיאום צמוד עם פרקליטות המדינות השונות בגרמניה או עם משרד הפרקליטות הפדרלית. הצוותים אמורים לאפשר זירוז תהליכי אכיפה והבאה לדין, בשיתוף עם רשויות האכיפה הגרמניות.

גם המשרד להגנת החוקה הקים "צוותי סייבר ניידים" (Mobile Cyber Teams) המורכבים ממומחי IT וממומחי מודיעין בעלי ניסיון בניתוח מתקפות קיברנטיות. צוותים אלה יכללו עובדים הבקיאים בשפות זרות ויסייעו בהתמודדות עם מתקפות קיברנטיות של גופי מודיעין זרים או מתקפות של ארגוני טרור.[6]

חיזוק צוותי **CERT** הקיימים והקמת צוותים נוספים לתגובות חירום

כאמור, צוות ה־CERT הפדרלי מסונף למשרד לאבטחת טכנולוגיות מידע ואחראי על סיוע לרשויות ולמפעילי תשתיות קריטיות, לעסקים, לארגוני המגזר הפרטי, לרשויות מקומיות ולמוסדות מחקר וידע. כמו כן, ה־CERT הפדרלי אחראי על שמירת קשר ותיאום עם צוותי CERT זרים ובין־לאומיים.[7]

ממשלת גרמניה אמורה להשקיע משאבים נוספים כדי להגדיל את צוות ה־CERT הפדרלי ולהרחיב את הידע והמומחיות של אנשיו. כמו כן אמורים לקום צוותי CERT חדשים.

חיזוק יכולות ההתרעה של שירות מודיעין החוץ הגרמני

שירות מודיעין החוץ הגרמני (BND) אחראי, בין השאר, על מעקב ורישום של ניסיונות מצד גורמים חיצוניים – מדינות, ארגוני טרור או פושעים – לתקוף

5 שם, עמ' 29.
6 שם.
7 שם, עמ' 34.

קיברנטית את התשתיות של גרמניה ושל המגזר הכלכלי והאזרחי בה. המעקב אחר ניסיונות תקיפה והתיעוד שלהם אמורים לאפשר ל־BND לבנות דפוס פעולה של התוקפים, וכך לספק התרעה מוקדמת בעת זיהוי פעילות חשודה מצידם.

ה־BND משתף פעולה עם מומחי IT ואנליסטים במטרה לבנות מערכת התרעה מוקדמת מפני מתקפות קיברנטיות. מערכת כזאת אמורה לזהות מתקפות מסוג זה מבעוד מועד, לנתח אותן ולבנות תמונת מצב של מפת האיומים. מאמצי הגילוי המוקדם מתבססים על מודיעין סיגינטי, הנאסף באמצעות ביצוע סריקות יזומות ברשת, כחלק ממדיניות המכונה Signals Intelligence Support to Cyber Defence.[8] פיתוח מערכת ההתרעה המוקדמת נגד מתקפות קיברנטיות החל ב־2014, ועד שנת 2020 יושקעו בפרויקט זה כ־300 מיליון אירו. הפרויקט מתבצע בשיתוף עם סוכנויות מודיעין של בעלות בריתה של גרמניה וצפוי לספק מענה גם לניסיונות ריגול ברשת.[9]

ה־BND משתמש בחיישנים המותקנים בסיבים אופטיים ברחבי העולם. אלה מקנים לשירות מודיעין החוץ הגרמני יכולת לעקוב אחר תעבורת מידע במדינות אחרות ולנטר מתקפות סייבר מבעוד מועד. שיטה זו גם מאפשרת איסוף מידע על תוכנות זדוניות והקמת מאגר מידע על כלי התקיפה.[10]

חיזוק המסגרות המשפטית והחוקית במרחב הקיברנטי

הממשלה הפדרלית הגרמנית פועלת לחזק את רשויות האכיפה והשיפוט במטרה להיאבק בפשיעה הקיברנטית. החיזוק יבוצע במספר דרכים:

- ראשית, הממשלה תהיה האחראית להקצאת משאבים לרשויות הרלוונטיות וכן לתוספת כוח אדם מיומן בתחומים של זיהוי מצבים, קרימינולוגיה במרחב הקיברנטי וזיהוי פלילי במרחב הדיגיטלי.
- שנית, הממשלה תסייע לרשויות הביטחון והאכיפה בפיתוח ובבנייה של מערכות ניתוח והערכה.
- שלישית, יושם דגש מיוחד על התאמה בין הטכנולוגיה לבין הסמכויות והאמצעים הניתנים לגופי האכיפה והשיפוט על פי החוק. פיתוח של שני התחומים זה לצד זה נועד למנוע פערים בין החוק ובין הטכנולוגיה.

---

8 שם, עמ' 32.

9 "300 Millionen für Frühwarnsystem gegen Cyber-Attacken", *Spiegel Online*, May 16, 2014, http://www.spiegel.de/netzwelt/netzpolitik/bnd-arbeitet-an-fruehwarnsystem-gegen-cyber-attacken-a-969899.html.

10 Frederik Obenmaier and John Goetz, "Geheimdienst verstärkt Kampf gegen Cyber-Angriffe", *Süddeutsche Zeitung*, May 9, 2014, http://www.sueddeutsche.de/politik/abwehr-von-schadsoftware-geheimdienst-plant-fruehwarnsystem-fuer-cyber-angriffe-1.1956067#redirectedFromLandingpage.

- רביעית, הממשלה תשים דגש על שיתוף פעולה בין הרשויות הגרמניות ובין מדינות אחרות בעולם. כמו כן, יושם דגש על חילופי מידע ועל חילופי ידע מקצועי וניסיון בין הרשויות הגרמניות ובין רשויות מקבילות להן במדינות אחרות, וכן בין הרמות הפדרלית והמקומית בתוך גרמניה עצמה.[11]

דוגמה לשיתוף פעולה שגרמניה רוצה לחזק היא שיתוף הפעולה עם האיחוד האירופי בכלל ועם גופים ספציפיים שלו, כמו סוכנות ביטחון הרשתות והמידע (ENISA) ומרכז הפשיעה הקיברנטית של יורופול.

חיזוק הסמכויות של גופים בגרמניה המתמודדים עם איומי סייבר מוצא ביטוי, בין השאר, בחיזוק סמכויותיהם של המשרד הפדרלי לפלילים ושל המשטרה הפדרלית בתחומי הפשיעה הקיברנטית, הריגול במרחב הקיברנטי ועוד. כמו כן, ממשלת גרמניה התחייבה לחזק את מרכז הפשיעה הקיברנטית הפועל במסגרת המשרד הפדרלי לפלילים ולהרחיבו. המטרה היא לחזק את יכולות החקירה וההערכה של המרכז וכן לעדכן את החוק הפלילי ולהחמיר את הענישה על פשיעה במרחב הקיברנטי.

כדי להתמודד עם הריגול במרחב הקיברנטי, יחוזקו סמכויותיו של המשרד להגנת החוקה. במסגרת זו ישופרו יכולותיו לקיים מעקב וניתוח יעילים יותר אחר דפוסי פעולה משתנים של טרוריסטים וגורמים קיצוניים ברשת.[12]

היערכות צבאית

שני צעדים ארגוניים משמעותיים ננקטו בתחום הביטחוני־צבאי במטרה לחזק את היערכותה של גרמניה להתמודדות עם האיום הקיברנטי: הקמת מחלקת הסייבר וטכנולוגיית המידע (CIT) תחת משרד ההגנה והקמת פיקוד הסייבר ומרחב המידע (CIR) העצמאי לצד זרועות הצבא. צעדים אלה נועדו לספק הגנה קיברנטית למערכות ה־IT הצבאיות, וכן לגבש אסטרטגיות צבאיות בתחום הסייבר כדי להפוך את כוחות הביטחון לרלוונטיים בעידן הדיגיטלי באמצעות הקניית יכולות קיברנטיות הגנתיות והתקפיות.

מחלקת הסייבר ושכנולוגיות המידע

בספטמבר 2016 הורתה שרת ההגנה של גרמניה, אורסולה פון דר ליין (Ursula von der Leyen) על הקמת מחלקה חדשה במשרד ההגנה, שתיקרא Cyber und Informationstechnik (CIT). לראש המחלקה החדשה מונה קלאוס הארדי מולק

11 "Cyber-Sicherheitsstrategie für Deutschland 2016", p. 30.

12 "Digitale-Agenda: Mehr Sicherheit im Cyberraum", *Bundesregierung*, 2014, https://www.digitale-agenda.de/Webs/DA/DE/Handlungsfelder/6_Sicherheit/6-5_Cyberraum/cyberraum_node.html.

(Klaus Hardy Muehleck),[13] והיא כוללת כ־130 משרות. מחלקת הסייבר וטכנולוגיות המידע תבנה את מערך האבטחה הקיברנטית הצבאי בהתאם לאסטרטגיית האבטחה הקיברנטית הלאומית. כמו כן, המחלקה תוביל את תהליכי ההתמקצעות של הצבא הגרמני בתחום אבטחת המידע ותהיה אחראית על הסייבר וה־IT בתחום הצבאי. מחלקת הסייבר וטכנולוגיות המידע כוללת שתי מחלקות משנה: אחת בברלין, שתעסוק במשילות בסייבר וב־IT, בתכנון ובאסטרטגיה בתחום טכנולוגיית המידע. משימותיה יהיו, בין השאר, מדיניות דיגיטלית בתחום הסייבר וניהול יוזמות IT. כמו כן, המחלקה תהיה אחראית לבנות את מערך ה־IT של משרד ההגנה והצבא הגרמני. מחלקת המשנה השנייה תוקם בעיר בון ומטרתה היא לתת שירותי IT ולעסוק ביישום ובתפעול שוטפים של מערכות ה־IT הצבאיות. תחומי אחריות נוספים של המחלקה הם הגנה על מערכות IT, הגנה קיברנטית פסיבית ואבטחת הצפנה.[14]

פיקוד הסייבר ומרחב המידע

פיקוד הסייבר ומרחב המידע (Cyber und Informationsraum – CIR) הוקם כחלק מהצבא הגרמני עוד בנובמבר 2015. משימתו הייתה לבחון את ההיבטים הארגוניים, את תחומי האחריות ואת המשימות של הצבא הגרמני (הבונדסוור) בתחומי הסייבר והמידע. באפריל 2017 החל ה־CIR לתפקד כפיקוד צבאי לכול דבר, וצפוי להפוך למִבצעי באופן מלא החל משנת 2021. בראש ה־CIR עומד גנרל בעל שלושה כוכבים. באוקטובר 2016 מונה לעמוד בראשו גנרל מאייר לודויג ליינהוס (Maier Ludwig Leinhos), שהכריז על הפיכת הפיקוד למבצעי בתחילת אפריל 2017.

פיקוד הסייבר ומרחב המידע החל את פעילותו עם צוות התחלתי של כ־260 איש, ועד יולי 2017 גדל מספר המשרתים בו לכ־13,500 איש. כוח האדם של CIR צפוי לגדול לכ־14,500 איש עד מועד ההפעלה המבצעית המלאה שלו ב־2021. 1,500 משרות ישוריינו לאזרחים.[15]

תפקידיו של CIR מוגדרים כהגנה פסיבית והגנה אקטיבית במרחב הסייבר והמידע. הצבא הגרמני מהווה מטרה רגישה למאות מתקפות קיברנטיות מדי יום, שמטרתן היא בראש ובראשונה לגנוב מידע ונתונים ולשבש מערכות נשק

13 לפני מינויו לתפקיד זה עבד מוֶלק כמנהל מערכות המידע של חברת "טיסנקרופ", כמנהל מערכות המידע של יצרנית הרכב "פולקסווגן" (2004־2011) וכאחראי טכנולוגיות מידע של יצרנית הרכב "אאודי" (2001־2004).

14 "Verteidigungsministerin stellt neue Cyber-Abteilung auf", *Bundesministerium der Verteidigung,* October 5, 2016.

15 "German Military to Unveil New Cyber Command as Threats Grow", *Reuters*, March 30, 2017, http://www.reuters.com/article/us-germany-military-cyber/german-military-to-unveil-new-cyber-command-as-threats-grow-idUSKBN1712MW.

נתמכות IT. מרכזיותו של הבונדסוור בברית נאט"ו תורמת אף היא להפיכתו ליעד משמעותי לפריצה. בשל רגישותו זו, מטרתו הראשונית של פיקוד הסייבר ומרחב המידע היא הגנה על הרשתות ועל מערכות ה־IT של הבונדסוור. הגנה פסיבית זו מתבצעת באמצעות ניטור, גילוי מוקדם, ניתוח והערכת נזקים, וכן נטרול האיום ויכולת סיוע בחזרה לשגרה. תפקידים נוספים של CIR הם הגנה על מוסדות ממשלה, גופים ציבוריים ותשתיות קריטיות מפני מתקפות קיברנטיות מצד גורמים זרים, כגון מדינות או ארגוני טרור, וכן מאבק בתעמולה, במידע כוזב ובחדשות כוזבות (Fake news).

בנוסף להגנה הפסיבית, בונה הבונדסוור יכולות התקפיות, אותן הוא מגדיר כ"הגנה אקטיבית". אלו מתבטאות ביכולת לאסוף מודיעין על רשתות ומערכות זרות ולשבש את פעילותן. יכולות התקפיות אלו נמצאות עדיין בתהליכי פיתוח תחת אחריותו של צוות "מבצעי רשתות מחשב" (Computer Network Operations – CNO). הצוות מורכב מכשמונים מומחים בוגרי מחלקות מדעי המחשב באוניברסיטה הצבאית של מינכן, המתמחים בחדירה לרשתות ולשרתים, בביצוע מניפולציות ובגרימת נזק.[16] צוות ה־CNO קיים מאז שנת 2009, אולם תחת פיקוד הסייבר ומרחב המידע הוא יורחב ויועבר ממחלקת המבצעים של הפיקוד האסטרטגי של הבונדסוור אל "מרכז מִבצעי סייבר" חדש, ויכולותיו בתחום סריקת רשתות, איסוף מודיעין ודימוי אויב יגדלו.

יכולות אלו של הצבא הגרמני מעוררות ויכוח ער בקרב מחוקקים בגרמניה וגוררות ביקורת מצד הציבור הגרמני, הסולד מפני שימוש בכוח וחושש מפני כניסה ל"מלחמת סייבר" או מרוץ חימוש קיברנטי, ולכן מגלה חשדנות כלפי הרעיון של מתן סמכויות וכוח נוספים לכוחות הביטחון. ואכן, היכולות ההתקפיות מהוות שינוי עמוק בתפיסת הביטחון הגרמנית, אשר הופך אותה ליותר פרו־אקטיבית מאשר בעבר.[17]

בניית מערך גיוס לפיקוד הסייבר ומרחב המידע

הבונדסוור משתף פעולה עם המשרד לרווחה ופיתוח בתחום גיוס כוח אדם חדש לפיקוד הסייבר ומרחב המידע. הכוונה היא ליצור מנגנון גיוס והעסקה שיכלול מסלולי קריירה למגויסים ויפעל בהתאם לדינמיות ולגמישות המאפיינות את שוק ה־IT. במטרה להגיע למספר היעד של המגויסים ולהכשיר כוח אדם יוזם

16 Christian Kahl, "Vom Kampf in der fünften Dimension", *Bundeswehr Journal*, May 3, 2013, http://www.bundeswehr-journal.de/2013/vom-kampf-in-der-funften-dimension.

17 Isabel Skierka, "Bundeswehr: Cyber Security, the German Way", *Observer Research Foundation*, October 20, 2016, http://www.orfonline.org/expert-speaks/bundeswehr-cyber-security-the-german-way/.

וגמיש מבחינה מחשבתית, נשקל הרעיון לפנות לאוכלוסיות ולקבוצות יעד שעד לא מזמן לא היו מועמדות לגיוס, ובהן אנשים שנמצאו לא מתאימים למסגרת צבאית, מועמדים מרקע של משפחות מהגרים, בעלי אזרחות כפולה, מועמדים שנשרו ממסגרות החינוך הפורמליות ומועמדים מרקע מקצועי אחר. מכשירי גיוס חדשים למציאת מועמדים מתאימים הם קיום תחרויות וטורנירים לגילוי כישרונות בתחום ה־IT, תחרויות סטארט־אפ, גיוס מועמדים מתחום הגיימינג וכן מתן מלגות ללימודים רלוונטיים.[18] בנוסף, הקים הבונדסוור מחלקת מחקר בשם Cyber Cluster באוניברסיטה הצבאית במינכן והשיק תוכנית לימודי תואר באבטחה קיברנטית, אותה צפויים לסיים כשבעים בוגרים כל שנה.[19]

הזירה הבין־לאומית

גרמניה רואה בזירה הבין־לאומית הזדמנות לחיזוק האבטחה הקיברנטית באמצעות שיתופי פעולה ויוזמות משותפות, אך גם כפלטפורמה לחיזוק הכלכלה והתעשייה הגרמנית, המבוססת ברובה על ייצוא. התייצבותה של גרמניה במרכז הזירה הבין־לאומית בתחום הסייבר וה־IT תורמת לחיזוק המוניטין והמעמד הפוליטי שלה ברחבי העולם.

במסמך האסטרטגיה משנת 2016 מתחייבת ממשלת גרמניה לפעול להתייצבותה בחזית המאמץ האזורי־אירופי והבין־לאומי כדי לבנות חסינות ויכולת התמודדות עם איומים קיברנטיים ולקבוע תקנים לאבטחה בתחום הסייבר.

את הזירות שבהן מתכוונת גרמניה לקדם את מדיניות האבטחה הקיברנטית ניתן לחלק לארבע: אירופה והאיחוד האירופי; נאט"ו; הזירה הבין־לאומית; שיתופי פעולה בילטרליים.

אירופה

ביטחון השוק האירופי וההמשכיות הסדירה של המסחר ביבשת הם אינטרסים עליונים של ממשלת גרמניה. עם צמיחת המסחר הדיגיטלי עולה גם חשיבותה של האבטחה הקיברנטית עבור השוק האירופי המשותף. ישנה חפיפה בין האינטרס הגרמני לאבטחת הכלכלה המקוונת, הרשתות ומערכות המידע שבהן נעשה שימוש, לבין האינטרס של הנציבות האירופית, ששמה לה למטרה ליצור אמון וביטחון בפרויקטים של האיחוד, ובהם השוק המשותף הדיגיטלי.

אינטרס נוסף של גרמניה הוא שמירה על זכויות אדם ועל פרטיות בשימוש באינטרנט. על רקע זה הודיעה ממשלת גרמניה על תמיכתה ברגולציה מטעם

18 "Abschlussbericht Aufbaustab Cyber- und Informationsraum", *Bundesministerium der Verteidigung*, April 2016, pp.31-33.

19 שם, עמ' 35־36.

הנציבות האירופית, אשר תסדיר אבטחה של העברת נתונים ומידע בתוך אירופה ותסייע לשמירה על הפרטיות ועל מסחר תקין.[20]

בנוסף, פועלת הממשלה לחזק את מעמדה של גרמניה במסגרת מדיניות הסייבר האירופית, וזאת באמצעות מעורבות גדלה והולכת שלה במדיניות החוץ והביטחון של האיחוד האירופי. ממשלת גרמניה גם תומכת בקידום מחקרים של חוקרים גרמנים בתחום אבטחת ה־IT ופועלת לקשר ביניהם ובין מוסדות מחקר מקבילים ברחבי אירופה, וכן לקדם את תעשיית ה־IT המקומית. חלק ניכר מקידום התעשייה הגרמנית, כמו גם הגדלת מעורבותה של גרמניה בעיצוב מדיניות האבטחה הקיברנטית של האיחוד האירופי, באים לידי ביטוי בתמיכה בשורת פרויקטים של האיחוד העוסקים בסוגיות חוקיות וטכניות הקשורות למרחב הסייבר, כגון שימוש בזיהוי אלקטרוני ובחתימות אלקטרוניות של עסקים ורשויות. שימוש זה יאפשר זיהוי אמין של המשתמש וכן שיתוף פעולה מלא עם הסוכנות האירופית לאבטחת רשתות ומידע (European Union Agency for Network and Information Security – ENISA).[21]

נאט"ו

מדיניות החוץ והביטחון של גרמניה רואה בנאט"ו את עמוד התווך עליו נשענת הברית האירו־אטלנטית. חברותה של גרמניה בברית מבטיחה הן את ביטחונה שלה והן את ביטחון אירופה. לפי האסטרטגיה הגרמנית, תפיסת הביטחון הקולקטיבי של נאט"ו תקפה גם במרחב הקיברנטי, ועל כן מוטל על הברית הצפון אטלנטית להתחזק גם במרחב זה, כפי שהוא עושה בים, באוויר וביבשה. גרמניה היא שותפה מרכזית ומובילה בתהליכי הבנייה של מערך האבטחה הקיברנטית של נאט"ו ושל מדיניות הרתעה אפקטיבית במרחב הקיברנטי אל מול איומי הלוחמה ה"היברידית", כלומר זו המשלבת לוחמה קינטית וקיברנטית.[22]

הזירה הבין־לאומית

גרמניה הציבה את עצמה כמובילת הדיונים בארגונים הבין־לאומיים, ובראשם הארגון לביטחון ושיתוף פעולה באירופה (Organization of Security and Cooperation in Europe – OSCE) והאו"ם, בנושאים הנוגעים לשמירה על החוק הבין־לאומי במרחב הקיברנטי, לסגירת פערים בחוק הבין־לאומי בתחום הסייבר, לפיתוח נורמות, רגולציות ועקרונות הנוגעים להתנהגות מדינית אחראית בתחום זה, וכן לחיזוק היכולות והסמכות של האו"ם במרחב הקיברנטי.

---

20 "Cyber-Sicherheitsstrategie für Deutschland 2016", p. 40.
21 שם.
22 שם.

תחומים נוספים שבהם גרמניה לוקחת חלק הם העלאת המודעות לסכנות במרחב הקיברנטי, הרחבת מסגרות שיתוף המידע סביב מתקפות ותקריות קיברנטיות, החרפת המענה הבין־לאומי והחמרת הענישה על ריגול כלכלי ועל מתקפות סייבר, וכן תמיכה אקטיבית בחיזוק הפיקוח על ייצוא טכנולוגיות היכולות לשמש להתנהגות תוקפנית במרחב הקיברנטי.[23]

קשרים בילטרליים

גרמניה פועלת לתמוך בשותפותיה ולסייע להן בבנייה של יכולות גילוי, מניעה ותגובה לתקריות קיברנטיות, וכן לתמוך בחיזוק תשתיותיהן הדיגיטליות. כחלק משאיפתה של גרמניה להיתפס כשחקן אמין בזירה הבין־לאומית, היא מעודדת גורמים שונים בזירה זאת לבצע רפורמות חוקיות בתחום הסייבר, לחתום על אמנות בתחום זה ולנקוט צעדים בוני אמון שיחזקו את הביטחון הקיברנטי.[24]

אתגרים והשלכות פוטנציאליות של ההיערכות הגרמנית

על אף ההיערכויות השונות, הגידול בכוח אדם והרחבת הסמכויות של הרשויות והגופים השונים, ממשיכה ממשלת גרמניה לעמוד בפני מספר אתגרים במרחב הסייבר. חלק מהם הן מגבלות חוקיות הנוגעות לשימוש ביכולות סייבר התקפיות ולשיתוף פעולה בין הצבא ובין גופי המודיעין והביון, ואחרים נוגעים לפערים בתחום כוח האדם. כמו כן, להיערכות הגרמנית בתחום הסייבר יש מספר השלכות פוטנציאליות על מדיניות החוץ והביטחון השאפתנית של גרמניה בזירה הבין־לאומית.

פערים חוקתיים הנוגעים לשימוש בכוח

כחלק מהריסון הצבאי שמאפיין את גרמניה מאז תום מלחמת העולם השנייה, החוקה הגרמנית קובעת שכול שימוש בכוח צבאי למטרות שאינן הגנתיות גרידא מחייב את אישור הפרלמנט. בדוח של משרד ההגנה הגרמני נכתב כי הצורך במנדט פרלמנטרי תקף גם במבצעים במרחב הקיברנטי.[25] בשל המורכבות של מרחב זה, שבו לא תמיד ניתן להבדיל בין צעדים הגנתיים ובין צעדים התקפיים, נשאלת השאלה כיצד ובאילו מקרים על הצבא לפנות לפרלמנט כדי לקבל את אישורו. נראה כי גם הסעיף בחוקה הדורש את אישור הפרלמנט למהלכים של הגנה אקטיבית או מכה מקדימה עלול להוות אתגר בפני ביצוע מבצעים קיברנטיים, במיוחד כשמדובר בביצועם באופן מהיר וחשאי. עד היום לא נמצאה הדרך לגישור על פערים אלה.

ביצוע מתקפות קיברנטיות מצריך מודיעין מדויק על הרשתות והמערכות של היעד וכן על נקודות התורפה שלו אותן ניתן לנצל. מודיעין כזה, כמו גם פעולות

23 שם, עמ' 41.
24 שם, עמ' 42.
25 "Abschlussbericht Aufbaustab Cyber- und Informationsraum", p. 5.

ריגול והכנה אחרות לצורך ביצוע מתקפות קיברנטיות, הם תחום הפעולה של שירותי מודיעין. לכן, הצבא הגרמני ייאלץ לשתף פעולה ומידע בנושא זה עם שירותי הביון והמודיעין של גרמניה. בעוד שבארצות הברית שיתוף פעולה כזה הוא מובן מאליו, מה גם ופיקוד הסייבר האמריקאי חולק את אותה הנהגה עם סוכנות הביטחון הלאומית (NSA) ועושה שימוש בנכסיה ובמודיעין שהיא מספקת, שיתוף פעולה כזה בגרמניה ניצב בפני מגבלות חוקיות חמורות. הממד המשפטי של שיתוף הפעולה בין גופי המודיעין ובין הצבא וגופי האכיפה בגרמניה חורג ממסגרתו של מאמר זה. עם זאת, ניתן לציין כי מתנהל ויכוח משפטי באשר לסוגי המידע שמותר לגופי הביון, ובפרט ל־BND, לשתף עם רשויות גרמניות אחרות.[26] בנוסף לכך, ה־BND כפוף למשרד הקנצלר, בעוד שהצבא הגרמני כפוף למשרד ההגנה, והמשרד להגנת החוקה כפוף למשרד הפנים. לא ברור לפיכך כיצד ניתן לקיים שיתוף פעולה ביניהם. זאת ועוד, לפי שעה טרם הוגדרה חלוקת הסמכויות בין שלושת הגופים בכול הנוגע לאיסוף מידע הנוגע למבצעים קיברנטיים.

אתגרים בגיוס כוח אדם מיומן

בעיה נוספת, שאינה מיוחדת דווקא לגרמניה, היא גיוס והכשרת כוח האדם המתאים למילוי ואיוש המשרות החדשות בצוותי ה־CERT, ובמיוחד בפיקוד הסייבר ומרחב המידע בבונדסוור. על אף הכרזת הצבא הגרמני כי פיקוד הסייבר כבר אויש על ידי חיילים שנבחרו מתוך ענפים אחרים של הצבא, הבונדסוור עודנו ניצב בפני האתגר של הקמת מאגר מילואים של הפיקוד החדש. במכתב שנשלח מהמשרד הפדרלי האחראי לחימוש ולהצטיידות הצבא[27] לחיילי מילואים מתחום ה־IT, הם התבקשו למסור שמות של עמיתיהם לתחום ה־IT האזרחי. כן נכתב בפניה כי הצבא זקוק להאקרים, למפתחי IT, למומחים לאבטחת IT, למְבַצעי בדיקות חדירות (Penetration testers) ועוד.[28]

מעֵבר לקושי בגיוס אנשי IT מוכשרים ומנוסים, סובל הבונדסוור מאחוזי גיוס נמוכים ומתדמית של מעסיק לא אטרקטיבי. כמו כן, נמתחה ביקורת על התוכניות השאפתניות של הצבא, תוך טענה כי הוא אינו גמיש מספיק וכי קצב ההכשרות,

26 Kai Biermann, "BND-Überwachung: Warum schickt der BND der Bundeswehr abgehörte Daten?", *Zeit Online,* March 18, 2015, http://www.zeit.de/politik/deutschland/2015-03/bnd-bundeswehr-daten-ueberwachung/komplettansicht.

27 The Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support.

28 Matthias Monroy, "Herausforderungen im Cyber- und Informationsraum: Bundeswehr sucht Tips für Aufbau einer Cyber-Reserve", *Netzpolitik,* April 26, 2016, https://netzpolitik.org/2016/herausforderungen-im-cyber-und-informationsraum-bundeswehr-sucht-tips-fuer-aufbau-einer-cyber-reserve/

הרכש וההצטיידות שלו אינו עולה בקנה אחד עם קצב היוזמה והחדשנות בשוקי החומרה והתוכנה, וכן עם קצב השינויים המהירים החלים במרחב הקיברנטי.[29]

תוכנית הלימודים האקדמית שהשיק הבונדסוור לצורך הכשרת אנשי IT היא צעד חיובי בכיוון הנכון, אך נוכח הצפי, לפיו כשבעים בוגרים אמורים לסיים את התוכנית כל שנה, ניתן להעריך כי יעבור זמן רב עד שהתוכנית תוכל לספק את צורכי הצבא. במצב זה קיים חשש שהבונדסוור ייאלץ לפנות לחברות קבלן פרטיות כדי שימלאו חלק ממשימותיו. אפשרות זו גורמת לחששות רבים של פגיעה בביטחון הלאומי, כפי שהודגם מספר פעמים בהדלפות מצד עובדי קבלן שפעלו עבור ה־NSA בארצות הברית.

הזדמנויות בזירה הבין־לאומית

שאיפותיה של גרמניה ורצונה למנף את מעמדה הבין־לאומי, כמו גם את כלכלתה ותעשייתה, אינן חדשות. בשנים האחרונות השתתפה גרמניה באופן פעיל ועקבי בפורומים בין־לאומיים שעסקו באבטחה קיברנטית ובטכנולוגיות מידע ותקשורת, כגון האו"ם, האיחוד האירופי, נאט"ו, פסגת ה־G–7, הארגון לביטחון ולשיתוף פעולה באירופה ועוד. כמו כן, גרמניה השתתפה בדיאלוגים בנושאי פיתוח ובניית יכולות קיברנטיות ולקחה חלק פעיל בדיוני קבוצת המומחים הממשלתיים של האו"ם (GGE) לקביעת נורמות התנהגות במרחב הקיברנטי.

פעילותה הבין־לאומית הבילטרלית של גרמניה התאפיינה ומתאפיינת בסיוע למדינות מתפתחות בתחום הסייבר, וכן בשיתופי פעולה בתחום זה עם מדינות מפותחות.[30] דוגמאות לשיתופי פעולה ודיאלוגים כאלה ניתן לראות, למשל, בדיאלוגים שנערכו בברלין עם משלחות מהודו,[31] בחתימת הסכם שיתוף פעולה עם

29 Nina Werkhäuser, "German Army Launches New Cyber Command", *Deutsche Welle*, April 1, 2016, http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517

30 Hathaway et al., "Germany: Cyber Readiness at a Glance", p. 13.

31 "Indo-German Intergovernmental Consultations in Berlin - Strengthening Cyber Cooperation", *German Missions in India*, May 31, 2017, http://www.india.diplo.de/Vertretung/indien/en/__pr/Politics__News/Merkel__Modi__2017__update2.html.

איגוד תעשיות הביטחון של אסטוניה,[32] ובהסכם שיתוף פעולה בתחום האבטחה הקיברנטית עם סינגפור.[33]

לצד מגמות אלו, הצפויות להימשך, נפתחו בפני גרמניה הזדמנויות נוספות בזירה הבין־לאומית: מדיניות ה"אמריקה תחילה" של הנשיא טראמפ, חוסר הבהירות המתמשך הנוגע לדרכה של ארצות הברית והתרחקותה היחסית מהאיחוד האירופי ומנאט"ו, לפחות בהשוואה לממשל אובמה, יכולים להוות הזדמנות עבור גרמניה למלא תפקיד מרכזי יותר בהנהגת מדינות המערב. באופן ספציפי, סגירת משרד המתאם לענייני אבטחה קיברנטית במחלקת המדינה של ארצות הברית ב־2017, שיכולה להיחשב כפגיעה ביכולותיה הדיפלומטיות של ארצות הברית בתחום האבטחה הקיברנטית, עשויה להוות הזדמנות עבור מדיניות החוץ השאפתנית של גרמניה.[34]

עזיבתה האפשרית של בריטניה את האיחוד האירופי תיצור, ככול הנראה, פערים בנושאי ביטחון ומודיעין באיחוד. הדבר נכון גם בתחום האבטחה הקיברנטית. הוואקום העלול להיווצר בעקבות עזיבתה של בריטניה – הנחשבת כשחקן מרכזי בתחום זה – עשוי לעודד את גרמניה לנסות למלא אותו ביכולותיה שלה. עם זאת, עזיבתה של בריטניה צפויה לפגוע לא רק באבטחה הקיברנטית, אלא במכלול שיתוף המידע בין מדינות האיחוד, ובכלל זה עם גרמניה.

סיכום

גרמניה רואה באיום הקיברנטי איום מרכזי ובעקבות זאת נערכת להגנה על כלכלתה, תעשייתה, כוחות הביטחון והתשתיות הקריטיות שלה. היא עושה זאת באמצעות שורה של פעולות במספר חזיתות: המשפטית, החוקתית, הצבאית, הפדרלית והמקומית. האסטרטגיה המקיפה של גרמניה שפורסמה בשנת 2016 מפרטת את הצעדים המרכזיים שנועדו לספק מענה לאיום הקיברנטי עליה. אסטרטגיה זו

32 "Cyber-Security Council Germany and Estonian Defence Industry Association sign cooperation agreement, agreeing upon fostering transnational cooperation in the area of cyber security together", *Cyber-Security Council Germany*, September 14, 2017, http://www.cybersicherheitsrat.de/data/PRESS-RELEASE-Cyber-Security-Council-Germany-and-Estonian-Defence-Industry-Association-sign-cooperation-agreement.pdf.

33 Prashanth Parameswaran, "What's in the New Singapore-Germany Cyber Pact?", *The Diplomat*, July 11, 2017, https://thediplomat.com/2017/07/whats-in-the-new-singapore-germany-cyber-pact/.

34 Morgan Chalfant, "Tillerson moves to close State cyber office", *The Hill*, August 29, 2017, http://thehill.com/policy/cybersecurity/348438-tillerson-moves-to-close-state-cyber-office.

תומכת בחיזוק ובהרחבה של הגופים והיחידות להגנה קיברנטית, וכן בהיערכות צבאית מחודשת, הכוללת הקמת גופים ייעודיים לתחום הסייבר.

בתחום ההיערכות הממשלתית, גרמניה שמה דגש על הרחבת הגופים הקיימים וחיזוק יכולותיהם. דוגמה בולטת לכך היא הרחבת המרכז הלאומי להגנה קיברנטית (Cyber A-Z), המשמש כגורם מקשר בין משרדי הממשלה השונים האחראים מבחינה חוקית על תחום הסייבר, וכן הקניית יכולות עצמאיות לגוף זה לצורך ניתוח, הערכה וגיבוש תמונת מצב, כמו גם הוספה של פלטפורמת אימון והדמיית מצבי חירום. דוגמאות נוספות הן חיזוק יכולות התגובה והיכולות המקומיות באמצעות סיוע פדרלי.

בזירה הצבאית, גרמניה הקימה את מחלקת הסייבר וטכנולוגיות המידע הפועלת תחת משרד ההגנה. המחלקה אחראית על תכנון האסטרטגיה הקיברנטית הצבאית ועל בניית מערך הסייבר של הבונדסוור. כמו כן, הוקם פיקוד הסייבר ומרחב המידע הצבאי (CIR), האחראי על הגנת הרשתות ומערכות ה־IT של הצבא ואמור להיות מצויד ביכולות הגנתיות והתקפיות. יכולותיו ההתקפיות הפוטנציאליות של הפיקוד מהוות שינוי מהותי במדיניות הגרמנית, שעד כה נמנעה משימוש בכוח ומבניית יכולות התקפיות, דבר שעשוי לעורר ביקורת ציבורית.

בזירה הבין־לאומית, נראה כי גרמניה רואה בשיתוף הפעולה הבין־לאומי והבילטרלי לא רק צעד אסטרטגי לחיזוק האבטחה הקיברנטית הלאומית, אלא גם הזדמנות למנף ולחזק את מעמדה הכלכלי והפוליטי בזירה האירופית מול מדינות שאיתן יש לה קשרים בילטרליים ומול ארגונים בין־לאומיים, וזאת על ידי הובלה ולקיחת חלק מרכזי במאמץ המשותף להתמודדות עם אתגרי סייבר. מיצובה של גרמניה כמעצמת סייבר מהווה ניסיון שלה לחזק את מעמדה הבין־לאומי, הפוליטי והדיפלומטי, וכן לחזק את התעשייה הטכנולוגית ואת הכלכלה הגרמנית מבוססת הייצוא.

גרמניה מצטרפת לשורה של מדינות אירופיות, ובכלל זה בריטניה וצרפת, החוששות מריגול, מגניבת מידע, מחוסר יציבות, מהשפעה חיצונית על הלך הרוח הציבורי ומהתערבות זרה בתהליכי הבחירות שלהן, ולכן הן בוחרות להשקיע מאמצים ומשאבים כדי להיות מוכנות להתמודדות עם איומים אלה. עם זאת, ישנם אתגרים חוקיים העומדים בפני התעצמותה של גרמניה בתחום הסייבר הצבאי, ובייחוד בתחום השימוש בנשק קיברנטי התקפי ובעקרונות ההגנה האקטיבית – חלק מתפקידיו של פיקוד הסייבר ומרחב המידע החדש. אתגרים נוספים הם בתחומי ההצטיידות וכוח האדם, אך אלה אינם מיוחדים לגרמניה. הצעדים החלקיים שננקטו כדי להתמודד עם אותם אתגרים הם מהלך בכיוון הנכון, אך אינם צפויים להוות פתרון מלא של הבעיה.

התהליך שעוברת גרמניה מעניין, בעיקר בשל עוצמתה ומרכזיותה בפוליטיקה ובכלכלה האירופית והבין־לאומית. ייתכן כי אירועים בעלי השפעה בין־לאומית, כגון מדיניות "אמריקה תחילה" של ממשל טראמפ, ידחקו בגרמניה להגדיל את הוצאות הביטחון שלה, הכוללות גם את תחומי הגנת הסייבר ולוחמת הסייבר. אירועים נוספים, כגון יציאת בריטניה מהאיחוד האירופי, צפויים לפגוע בביטחונה של גרמניה בכלל ובאבטחה הקיברנטית שלה בפרט, וזאת נוכח העובדה שביטחונה קשור לביטחון האיחוד האירופי כולו.

תהליך מעניין נוסף הוא השינוי העמוק שחל בתפיסת הביטחון הגרמנית, שעל אף האתגרים החוקיים מתבססת יותר ויותר על הגנה אקטיבית ואמצעים התקפיים. זהו שינוי גדול עבור מדינה שנמנעה בשבעים השנים האחרונות משימוש בכוח. עם זאת, שינוי זה צפוי להמשיך להיתקל במתנגדים רבים, הן מקרב הציבור והן מקרב המחוקקים בגרמניה, דבר שיקשה על מימושו.