מכון ירושלים לאסטרטגיה ולביטחון
The Jerusalem Institute
for Strategy and Security

תכנון רב-שנתי לבניין כוח

גבי סיבוני
סיימון ציפיס

מכון ירושלים לאסטרטגיה ולביטחון
The Jerusalem Institute
for Strategy and Security

תכנון רב-שנתי לבניין כוח

גבי סיבוני
סיימון ציפיס

מאי 2026
סיוון התשפ״ו

תכנון רב-שנתי לבניין כוח

1 מבוא

כוח תכנון רב-שנתי לבניין כוח מהווה כיום אחד האתגרים המורכבים והקריטיים ביותר העומדים בפני ארגוני ביטחון וביטחון פנים בכל העולם. בעידן שבו איומים היברידיים, טכנולוגיות מתפתחות בקצב מהיר, אי-ודאות גאו-פוליטית ותקציבים מוגבלים הם נורמה – יכולתו של ארגון לבנות, לשדרג ולתחזק יכולות מבצעיות באופן שיטתי, ארוך טווח וממוקד-תוצאות קובעת לא רק את יעילותו, אלא את עצם הרלוונטיות שלו.

בניין כוח אינו עוד תהליך טכני של מחקר ופיתוח, רכש ציוד או גיוס כוח אדם. הוא תהליך הכולל שילוב הדוק בין תפיסת הפעלה, דוקטרינה, טכנולוגיה, כוח אדם, ארגון, תשתיות ומדיניות. הוא מחייב יכולת צפייה קדימה, זיהוי אותות חלשים, ניתוח פערים, הקצאת משאבים מיטבית והתאמה מתמדת למציאות משתנה. ארגונים שמצליחים לבצע תהליך זה בצורה מובנית זוכים לגמישות אופרטיבית, יתרון תחרותי והיערכות טובה יותר לאתגרים עתידיים.

מסמך זה בוחן את התחום מנקודות מבט השוואתיות. הפרק ראשון מציג מודלים מרכזיים מתחום הביטחון האמריקאי – JCIDS, PPBE, DOTMLPF-P, Capability-Based Planning ותכנון כוח מודולרי – המהווים כיום את הבסיס לתכנון ארוך טווח במדינות רבות. מודלים אלה מדגישים מעבר מתכנון מבוסס איומים לתכנון מבוסס יכולות, שילוב בין מדיניות, תקציב וביצוע, וגישה הוליסטית הכוללת את כל רכיבי הכוח.

הפרק שני מציג מקרי בוחן משירותי ביטחון פנים מובילים: MI5 הבריטי, BfV הגרמני, FSB הרוסי וה-FBI האמריקאי. דרך ניתוח השוואתי של תהליכי התכנון, הערכת איומים, גיוס והכשרת כוח אדם, שילוב טכנולוגיה ויחסי גומלין עם הרשות המבצעת והמחוקקת, עולים הבדלים מהותיים הנובעים מתרבות ארגונית, מסגרת חוקית ומאפייני המשטר. בעוד שבמדינות דמוקרטיות ליברליות (בריטניה, גרמניה) הדגש הוא על פיקוח, שקיפות והגנה על זכויות, ברוסיה בולטת השפעת הפוליטיזציה והריכוזיות.

הפרק שלישי עוסק בכלים מתקדמים של העידן הדיגיטלי – בינה מלאכותית, סריקת אופק (Horizon Scanning) וניתוח חיזוי (Predictive Analytics). סריקת אופק בשילוב AI, הכוללת חמישה שלבים מוגדרים (הגדרת היקף, איסוף נתונים, זיהוי אותות חלשים, ניתוח והערכה, סינון והמלצות), מאפשרת לארגונים לזהות מגמות וסיכונים מוקדם יותר, להפחית הטיות אנושיות ולשפר את איכות קבלת ההחלטות.

בחלק האחרון מוצע מודל לתכנון רב-שנתי לבניין כוח, המותאם לצרכים של ארגוני ביטחון פנים. המודל מבוסס על הבחנה ברורה בין הפעלת הכוח (פעולות חיצוניות) לבין בניין הכוח (פעולות פנימיות), ומציע תהליך תלת-שנתי מחזורי הכולל הערכת מצב, גיבוש אתגרים, בניית תפיסות מענה, פירוק לפרויקטים והטמעה בתוכנית עבודה שנתית. המודל מדגיש שימוש בכלי AI לסריקת אופק, ומדידת תפוקות כבסיס

להערכה. המסמך מדגיש כי בניין כוח מוצלח דורש איזון עדין בין שלושה צירים: צורך מבצעי, יכולת טכנולוגית-ארגונית ואילוצים תקציביים-משפטיים. הוא מראה כי ארגונים שמצליחים לשלב בין גישה הוליסטית (כגון DOTMLPF-P), תכנון מבוסס יכולות וכלים דיגיטליים מתקדמים – מצליחים להתמודד טוב יותר עם אי-ודאות.

בעולם שבו המהפכה הטכנולוגית, האיומים והלחץ התקציבי רק ילכו ויתגברו, תכנון רב-שנתי לבניין כוח אינו עוד "תהליך מנהלי" אלא יתרון מרכזי. המסמך מבקש לתרום להעמקת ההבנה ולפיתוח גישות מעשיות שתאפשרנה לארגונים להתאים עצמם במהירות וביעילות למציאות המשתנה.

2 מודלים לתכנון בניין כוח

פרק זה מתייחס לכמה מודלים לבניין כוח בארגוני ביטחון וביטחון פנים. תפיסת בניין הכוח הנהוגה בצה"ל (בעיקר תפיסת התכנון הרב-שנתי) אינה מפורטת כאן, והיא מנותחת במסגר ההמלצות לתהליכי תר"ש בסוף מסמך זה.

JCIDS 2.1

JCIDS (Joint Capabilities Integration and Development System) – מערכת שילוב ופיתוח יכולות משותפות – היא התהליך העיקרי של משרד ההגנה האמריקאי (DoD – Department of Defense, ששמו שונה לאחרונה למשרד המלחמה) לזיהוי, הערכה, אימות וקביעת סדרי עדיפויות של דרישות ופערים בתכנון יכולות צבאיות של ארה"ב.[1]

המטרה מרכזית של המערכת היא תרגום הנחיות של הדרג המדיני (למשל תפיסת הגנה לאומית) ליישומן הלכה למעשה, באמצעות קביעת צרכים ויכולות ספציפיים והתאמתם. ההנחיות יכולות להתבצע על ידי פתרונות טכנולוגיים, כגון מערכות חדשות, שינויי מדיניות/דוקטרינה, גיוס והכשרת כוח אדם או התאמות ארגוניות. היא מדגישה את הצורך בשיתוף פעולה בין אגפים שונים בתוך משרד ההגנה בשילוב עם תהליך הרכש של משרד ההגנה.[2]

האלמנטים המרכזיים של המערכת הם: הערכה מבוססת יכולות (CBA – Capabilities-Based Assessment) המנתחת תחומים פונקציונליים, צרכים, פערים וסיכונים; דוח יכולות ראשוני (ICD), ומסמך פיתוח יכולות (CDD); פיקוח על תהליך היישום המנוהל על ידי מועצת פיקוח משותפת על דרישות (JROC) תחת יו"ר המטות המשולבים, בהשתתפות של נציגי אגפים רלוונטיים כולל מפקדות ומרכיבים אחרים של משרד ההגנה.[3]

JCIDS היא מערכת של משרד הביטחון/צבא ואינה בשימוש ישיר של סוכנויות ביטחון פנים כמו DHS, FBI או FEMA לתכנון פנימי ארוך טווח. לסוכנויות אלו יש תהליכים משלהן (למשל DHS משתמש בוועדה

1 Congressional Research Service. 2024. "Defense Primer: Joint Capabilities Integration and Development System (JCIDS)". IN FOCUS 3 (November), https://www.congress.gov/crs_external_products/IF/PDF/IF12817/IF12817.3.pdf

2 Joint Chiefs Of Staff. 2025. Joint Capabilities Integration and Development System, https://web.archive.org/web/20070204073933/http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf

3 Neenan, Alexandra G. (US Congress Webpage). 2024. "Defense Primer: Joint Capabilities Integration and Development System (JCIDS)". November 14, https://www.congress.gov/crs-product/IF12817

לדרישות ספציפיות משותפות לתכנון ויישום דרישות ליכולות נדרשות).[4] עם זאת, מערכת התכנון ממלאת תפקיד עקיף התומך בהקשרים של ביטחון פנים, כגון תיאום בין-סוכנויות, בייחוד במערכי הגנת פנים, תמיכה אזרחית והיערכות למצבי חירום. המערכת מאפשרת לסוכנויות ביטחון פנים לתאם עם משרד הביטחון את היכולות המשותפות כמו תקשורת, אבטחת סייבר או מערכות זיהוי.[5]

ה-DHS וסוכנויות אחרות הפיקו לקחים מגישות בסגנון JCIDS לניתוח פערים, קביעת סדרי עדיפויות, ניתוח סיכונים והיערכות.[6] מאמצים משותפים בתרחישים הכוללים תמיכה ביטחונית של רשויות אזרחיות מסייעים להבטיח כי יכולות צבאיות משתלבות ביעילות עם צורכי ביטחון פנים אזרחיים. מודל ה-JCIDS נותן מענה לדרישות של הצבא בשיתוף עם גופי ביטחון אחרים, כאשר בעקיפין הוא מאפשר ממשק עם תכנון פנימי באמצעות שיתוף פעולה בין-סוכנותי, ופחות יעיל ככלי מרכזי עבור סוכנויות אזרחיות או שירותי ביטחון פנים.

PPBE 2.2

PPBE (Planning, Programming, Budgeting, and Execution)—תכנון, תכנות, תקצוב וביצוע — הוא תהליך מובנה ומחזורי של הקצאת משאבים וניהול, המשמש סוכנויות ביטחון פנים אמריקאיות, ובראשן משרד ביטחון המולדת (Department of Homeland Security DHS). הוא מבוסס על מודל של מערכת מסורתית של משרד המלחמה, אך מותאם למשימות ביטחון פנים.[7]

המטרה של תהליך ה-PPBE היא לסייע לסוכנויות לתרגם סדרי עדיפויות של ביטחון לאומי (למשל לוחמה בטרור, אבטחת גבולות, אבטחת סייבר, תגובה לאסונות) לתוכניות ויכולות ממומנות ומתוקצבות. המטרה היא להבטיח שמשאבים יהיו מסונכרנים עם יעדים ארוכי טווח, אילוצים תקציביים ותוצאות ביצועים במסגרת רב-שנתית.[8]

התהליך נפרס לארבעה שלבים: שלב תכנון, הכולל פיתוח חזון ארוך טווח המבוסס על הנחיות דרג ממונה (למשל תוכנית רב-שנתית של ה-DHS, תפיסת ביטחון לאומי), זיהוי איומים, סדרי עדיפויות, פערים ביכולות, צורכי השקעה ותקצוב; שלב התכנות (Programming), המתרגם תוכניות לדרישות משאבים ספציפיות (כוח אדם, ציוד, תוכניות) המשתרעות על פני שנים מספר. הסוכנויות מגבשות תוכניות, ומפיקות המלצות. שלב זה מסתיים בהחלטות קובעות כמו החלטת הקצאת משאבים של ה-DHS; שלב התקצוב, המתמקד בטווח הקרוב (בדרך כלל שנת הכספים הקרובה). הוא משפר את דרישות התוכנית לבקשות תקציב מפורטות, מצדיק אותן בפני OMB (Office of Management and Budget) והקונגרס של ארה״ב, ומבטיח עמידה בבקרות התקציביות;[9] ושלב הביצוע, המתרכז ביישום התקציב שאושר, ביצוע

4 G.A.O US Government Accountability Office (GAO-23-106125). 2023. "Homeland Security: Joint Requirements Council Needs Leadership Attention to Improve Effectiveness". August 30, https://www.gao.gov/products/gao-23-106125

5 MAJ Kevin P. Wilson. 2007. "Determining Communication Shortfalls for Homeland Defense". *Strategic Insights* VI (6), https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Determining%20Communication%20Shortfalls%20for%20Homeland%20Defense.pdf

6 Sharon Caudle. 2025. "Homeland Security Capabilities-Based Planning: Lessons from the Defense Community". *The Journal of the NPS Center for Homeland Defense and Security* I (August), https://www.hsaj.org/articles/178

7 Transportation Security Administration. 2017. *To Enhance Mission Performance, TSA Is Committed to Promoting a Culture Founded on Its Values of Integrity, Innovation and Team Spirit*, https://www.tsa.gov/sites/default/files/foia-readingroom/planning_programming_budgeting_and_execution_500.1.pdf

8 Department of Homeland Security. 2019. *Planning, Programming, Budgeting, And Execution*, https://www.dhs.gov/sites/default/files/publications/mgmt/planning-and-budgeting/mgmt-dir_101-01-planning-programming-budgeting-execution_revision-01.pdf

9 Department of Homeland Security. 2019. *Planning, Programming, Budgeting, And Execution*, https://www.dhs.gov/sites/default/files/publications/mgmt/planning-and-budgeting/mgmt-dir_101-01-planning-programming-budgeting-execution_revision-01.pdf

פעולות, ניטור ביצועים ומדידת תוצאות. שלב זה מספק משוב למחזורי תכנון עתידיים (למשל באמצעות ביקורות, מדדים ולקחים שנלמדו).[10]

מאפיינים עיקריים של תהליך זה הם מחזוריות וחפיפה. הוא פועל מדי שנה אך משתרע על פני שנים מספר, ומאפשר יישור מתמשך של תוכנית פעולה ומשאבים. הוא משולב ומקשר מדיניות עם אסטרטגיה, החלטות לגבי משאבים והערכת ביצועים.[11] ה-DHS מיישם את ה-PPBE באמצעות הנחיות לניהול מערך המשימה העיקרית שלו על כל רכיביו. ה-PPBE משמש כמסגרת מרכזית להפיכת כוונות ארוכות טווח בביטחון פנים לתוכניות מעשיות וממומנות תוך קידום יעילות ואחריות.[12]

DOTMLPF-P 2.3

DOTMLPF-P היא מסגרת לתכנון ארוך טווח וניתוח יכולות שפותחה במקור על ידי משרד ההגנה האמריקאי (בשימוש במערכת שילוב ופיתוח יכולות משותפות – JCIDS) ואומצה על ידי ארגוני ביטחון שונים, כולל סוכנויות ביטחון פנים/מולדת (למשל ה-DHS[13]). אלו מרכיבי הגישה:

- D דוקטרינה – תפיסה להפעלת הכוח, עקרונות יסוד, מדיניות.
- O ארגון – מסגרות, יחידות ופיקוד.
- T אימון – אימונים, תרגילים והטמעה.
- M חומר – אמצעי לחימה, ציוד, מערכות, טכנולוגיה.
- L מנהיגות וחינוך – פיתוח מנהיגות והכשרה.
- P כוח אדם – גיוס והכשרת כוח אדם.
- F מתקנים – תשתיות, בסיסים ומשאבים פיזיים.
- P מדיניות – חוקים, כללים, תקנות, הנחיות והנחיות מקיפות.[14]

בתכנון רב-שנתי עבור סוכנויות כמו אכיפת חוק, אבטחת גבולות, ניהול חירום או שירותי מודיעין, ה-DOTMLPF-P משמש כרשימת תיוג או בידוק הוליסטית להערכת יכולות קיימות, זיהוי פערים וחולשות, ופיתוח פתרונות מאוזנים בעת התמודדות עם איומים (למשל טרור, סיכוני סייבר, אסונות טבע או אתגרי גבולות). הגישה מדגישה כי רכישת טכנולוגיה (חומרים) חדשים היא לעיתים רחוקות פתרון מספיק.

שיפורים בני קיימא דורשים בדרך כלל שינויים מתואמים בכל האלמנטים. לדוגמה, ציוד מעקב חדש חייב להיות נתמך בדוקטרינה מעודכנת, תוכניות הכשרה, התאמות ארגוניות, אישורי מדיניות ומתקנים וכוח אדם מתאימים.[15] מסגרת זו מקדמת חשיבה מקיפה ולא מבודדת רק לפיתוח יכולות, ניתוח פערים והקצאת משאבים. היא מסייעת למנהיגים בכירים להבטיח שהתכנון ניתן ליישום ויעיל על פני מלוא ספקטרום הצרכים הארגוניים.

---

10 Transportation Security Administration. 2017. *Planning, Programming, Budgeting, And Execution*, https://www.tsa.gov/sites/default/files/foia-readingroom/planning_programming_budgeting_and_execution_500.1.pdf

11 Megan McKernan, Raphael S. Cohen, Michael Simpson, Ryan Consaul, and Stephanie Young. 2024. "Planning, Programming, Budgeting, and Execution in Comparative Organizations". *RAND* 3 (January), https://www.rand.org/pubs/research_reports/RRA2195-3.html

12 Megan McKernan, Raphael S. Cohen, Michael Simpson, Ryan Consaul, and Stephanie Young. 2024. "Planning, Programming, Budgeting, and Execution in Comparative Organizations". *RAND* 3 (January), https://www.rand.org/pubs/research_reports/RRA2195-3.html

13 AcqNoted (The Defence Acquisition Encyclopedia). 2024. "DOTMLPF-P Analysis". January 18, https://acqnotes.com/acqnote/acquisitions/dotmlpf-analysis

14 AcqNoted (The Defence Acquisition Encyclopedia). 2024. "DOTMLPF-P Analysis". January 18, https://acqnotes.com/acqnote/acquisitions/dotmlpf-analysis

15 John Boggs (Fortitude Consulting LLC). 2015. "Strategic Leaders: How's Your DOT-ML-PF-P?". https://fortitudeconsult.com/insights/articles/strategic-leaders-hows-your-dot-ml-pf-p

גישה זו קרובה לגישה הנוהגת בצה"ל בתהליכי בניין כוח, כשהיא מחייבת ראשית לכול גיבוש תפיסת פעולה (דוקטרינה) שעל בסיסה נשען כל התהליך. תפיסה זו מהווה מצפן שמאפשר לוודא שכל תהליכי בניין הכוח נגזרים מתוך תפיסת הפעלת הכוח.

במקום לשאול "עם אילו איומים אנו צפויים להתמודד?" ה-CBP שואל: "לאילו יכולות אנו זקוקים כדי לבצע בהצלחה את משימותינו במגוון רחב של תנאים אפשריים?"

CPB 2.4

תכנון מבוסס יכולות (CBP Capability-Based Planning) – גישת תכנון שמשתמשות בה סוכנויות ביטחון פנים (כגון משטרה, שירותי מודיעין, משמר הגבול או ארגוני ביטחון פנים) ומתמקדת בפיתוח ותחזוקה של יכולות ספציפיות הנדרשות להשגת יעדי משימה, במקום לתכנן כתגובה לאיומים או תרחישים ספציפיים וצפויים.

הרעיון המרכזי הוא שבמקום לשאול "עם אילו איומים אנו צפויים להתמודד?" (תכנון מבוסס איומים) ה-CBP שואל: "לאילו יכולות אנו זקוקים כדי לבצע בהצלחה את משימותינו במגוון רחב של תנאים אפשריים?". המאפיין העיקרי של הגישה בהקשר של ביטחון פנים הוא שהוא ממוקד יכולות: מגדיר יכולות במונחים של אנשים, תהליכים, טכנולוגיה, ציוד, הכשרה וארגון, למשל "תגובה מהירה לאירועי נפגעים המוניים", "מיזוג בין מודיעין לאיומי סייבר", "ניהול קהל בסביבה עירונית" או "שיתוף מידע מאובטח בין סוכנויות".

עצם הגישה היא "ללא תלות בתרחיש" – Scenario-independent. יכולות מתוכננות להיות גמישות וניתנות להתאמה על פני אירועים עתידיים מרובים סבירים, כולל סיכונים לא ידועים מראש או מתפתחים תוך כדי (טרור, אסונות טבע, מתקפות סייבר, מרי אזרחי, מגפות וכו').

בניתוח פערים הסוכנויות מעריכות יכולות קיימות מול אלו הנדרשות, מזהות ליקויים (פערים) ובונות סדר עדיפויות להשקעות ותקצוב לסגירת הפערים. הגישה מכוונת לזיהוי וקטלוג סיכונים ולתוצאות מרביות בטיפולם. התכנון מונע על ידי תוצאות רצויות ברמות סיכון מקובלות, ולא על ידי תוכניות נוקשות המתמקדות באויב או בתרחישים ספציפיים. תיעדוף משאבים, המהווה חלק אינטגרלי של הגישה, מסייע להצדיק תקציבים והקצאת משאבים על ידי קישור השקעות ישירות ליכולות ניתנות למדידה.

הגישה מטפלת טוב יותר בחוסר ודאות ובאיומים מורכבים והיברידיים הנפוצים בביטחון פנים; מקדמת יכולת פעולה משותפת בין סוכנויות שונות (אכיפת חוק, מודיעין, שירותי חירום, שיטור וכו'); תומכת תכנון ארוך טווח תוך שמירה על תגובה לסביבה משתנה.

דוגמה ליישום הגישה: סוכנות משטרה לאומית המשתמשת ב-CBP עשויה להחליט שהיא זקוקה ל"יכולת התרעה מוקדמת". לאחר מכן היא תבנה את כלי המודיעין הדרושים, הכשרת אנליסטים, פרוטוקולים בין-סוכנויות ומסגרת משפטית, ללא קשר לשאלה האם האיום הנוכחי קשור לקיצוניות על רקע דתי, או על רקע פוליטי כגון ימין או שמאל קיצוני, או קיצוניות ממניעים אחרים. ה-CBP מעביר כאמור את התכנון מ"תכנון נגד איומים" ל"תכנון יכולת לפעול ביעילות מרבית" על פני מגוון רחב של אתגרי ביטחון. הוא נמצא בשימוש רחב על ידי ארגונים כמו משרד ביטחון המולדת של ארה"ב (DHS), סוכנויות ביטחון פנים אירופאיות וגופי הביטחון הפנימיים של חברות בנאט"ו.

2.5 תכנון בניין כוח מודולרי – Modular Force design

תכנון כוח מודולרי מקורו בעיקר כרעיון של צבא ארה"ב מתחילת-אמצע שנות ה-2000. הוא עבר ממבנים גדולים, המתמקדים בדיוויזיה, לצוותי קרב חטיבתיים (BCT) קטנים יותר, סטנדרטיים ועצמאיים, ויחידות תמיכה, המתפקדות כ"אבני בניין" מתחלפות (מודולים).[16] מודולים אלה (למשל BCT של חיל רגלים, BCT של סטרייקר/Stryker או BCT של נשק כבד/משוריין) כוללים יכולות לחימה אורגניות, תמיכה בלחימה ויכולות התקיימות (בר קיימא). ניתן להתאים אותם, לפרוס אותם ולשלב אותם במהירות למשימות ספציפיות ללא תלות רבה במפקדות גבוהות יותר לצורך הגדלת כוחות. היתרונות העיקריים כוללים גמישות רבה יותר, יכולת פריסה, קיימות לפעולות ממושכות ויכולת לייצר יותר חבילות כוח סיבוביות רוטציוניות.[17]

עקרונות ליבה של תכנון כוח מודולרי הם: סטנדרטיזציה – תכנון יחידות עקבי לשילוב ואימון קלים יותר; עצמאות – יחידות הנושאות את המרכיבים המרכזיים של עצמן (כגון מודיעין, לוגיסטיקה, מהנדסים, כוחות צבא); מדרגיות והתאמה אישית – שילובים של "חבר והפעל" לצורכי המשימה (למשל יחידת BCT אחת + מודולים של תמיכה לאיום ספציפי); מוכנות סיבובית (רוטציונית) – תומכת במחזורים צפויים כמו ARFORGEN (Army Force Generation – יצירת כוחות צבא) לפעולות מתמשכות.[18] גישה זו התייחסה לדרישות שלאחר המלחמה הקרה לפעילות משלחות אופרטיביות נגד אירועי התקוממות ומקרי חירום מגוונים.

תכנון מודולרי תומך בתכנון מבוסס יכולות ולא במבנים ספציפיים לאיום. מתכננים מעריכים את ההשפעות הנדרשות (למשל אבטחת גבולות, תגובה לאסונות, לוחמה בטרור), ובונים חבילות כוח מודולריות. בבניית כוח, זה מאפשר צמיחה הדרגתית: הוספת יחידות סטנדרטיות, איזון מחדש של מרכיבים פעילים, כוח מילואים, והקצאת מיומנויות מיוחדות ממוקדות (למשל יותר כוחות צבא או גופים אזרחיים) ללא תכנון מחדש מלא.[19]

דוגמאות בהקשרים של ביטחון פנים ויבשה: אימוץ ישיר ללא התאמה של "תכנון הכוח המודולרי" של הצבא מוגבל ביישום על ידי סוכנויות או מוסדות פנים אזרחיים (למשל רכיבי DHS כמו CBP, ICE, FEMA או אכיפת חוק מקומית), מכיוון שאלה נותנים עדיפות לשיטור, אבטחת גבולות ותגובת חירום על פני מערכי לחימה. עם זאת, עקרונות מודולריים מיושמים או מקבילים בכמה דרכים: תמיכה של צבא ארה"ב בהגנה/ביטחון פנים (למשל תמיכה ביטחונית ברשויות אזרחיות – DSCA). יחידות BCT מודולריות או כוחות משימה מותאמים אישית מספקות תמיכה הניתנת להרחבה לאסונות טבע ולאירועי רב-נפגעים, לאבטחת גבולות או לאי שקט (מרי) אזרחי. מודולים עצמאיים נפרסים במהירות עם אלמנטים לוגיסטיים ופיקודיים אורגניים.

16 William M. Donnelly (US Army Center for Military History). 2007. "Transforming an Army at War: Designing the Modular Force, 1993-2005", https://history.army.mil/Publications/Publications-Catalog/Transforming-an-Army-at-War

17 Stuart Johnson John E. Peters, Karin E. Kitchens, Aaron L. Martin, Jordan R. Fischbach. 2012. "A Review of the Army's Modular Force Structure". RAND, March 16, https://www.rand.org/pubs/technical_reports/TR927-2.html

18 Stuart E. Johnson, Aaron Martin, John E. Peters, and Karin E. Kitchens. 2011. "A Review of the Army's Modular Force Structure". In RAND, https://apps.dtic.mil/sti/tr/pdf/ADA545348.pdf

19 Raymond T. Odierno (US Army). 2013. "CSA's Strategic Intent: Delivering Strategic Landpower in an Uncertain World". February 6, https://www.army.mil/article/95729/csas_strategic_intent_delivering_strategic_landpower_in_an_uncertain_world

לסיכום, תכנון כוח מודולרי (או עקרונותיו) משפר את הזריזות בסביבות לא-ודאיות על ידי התייחסות לכוחות כאל ערכות כלים הניתנות להרכבה ולא בהיררכיות נוקשה. עבור סוכנויות פנים/ארציות הוא משמש כבסיס לתכנון אזרחי-צבאי היברידי, בניית תגובה מהירה וגישות כלל-ממשלתיות.

תכנון כוח מודולרי משפר את הזריזות בסביבות לא-ודאיות על ידי התייחסות לכוחות כאל ערכות כלים הניתנות להרכבה ולא בהיררכיות נוקשה.

3 תכנון בניין כוח בשירותי ביטחון פנים – מקרי בוחן

3.1 MI5 – בריטניה

ה-MI5 הינו סוכנות המודיעין וביטחון הפנים של בריטניה, האחראית על הגנה מפני איומים כמו טרור, ריגול, חבלה ופעולות שמטרתן לערער את הדמוקרטיה הפרלמנטרית הבריטית. היא אינה סוכנות "ביטחון פנים" במובן של ארגון צבאי למחצה או אכיפת חוק כמו שירות הביטחון האמריקאי; היא מתמקדת באיסוף מודיעין, ניתוח, שיבוש (לעיתים קרובות בשיתוף פעולה עם המשטרה), ייעוץ ביטחוני לממשלה ופעילות מנע.[20]

חלק ניכר מהתכנון ארוך הטווח הפנימי המפורט והמתודולוגיות המבצעיות של ה-MI5 מסווגות מסיבות ביטחון לאומי. מידע ציבורי מגיע מהאתר הרשמי של הארגון, מדברים פומביים של ראש הסוכנות, מדוחות פיקוח פרלמנטריים (למשל ועדת המודיעין והביטחון Intelligence and Security Committee – ISC), מהחקיקה, כמו חוק שירותי הביטחון משנת 1989 וחוק סמכויות חקירה, ומדיווחים היסטוריים. להלן תיאור התהליך של תכנון בניין כוח של הסוכנות על סמך מקורות זמינים.[21]

עבודת ה-MI5 תואמת את סדרי העדיפויות הרחבים יותר של בריטניה בתחום הביטחון הלאומי:

דרישות וצורכי מודיעין לאומיים וסדרי עדיפויות ממשלתיים הכוללים סדרי עדיפויות הנקבעים או המושפעים על ידי הממשלה באמצעות ועדת המודיעין המשותפת (Joint Intelligence Committee – JIC) ופיקוח משרדי (בעיקר שר הפנים). אלה ניזונים מהתכנון של ה-MI5. מתודולוגיית CONTEST (Counter-Terrorism Strategy and National Security Strategy) ללוחמה בטרור ותפיסת הביטחון הלאומית של בריטניה מספקות מסגרות מקיפות.[22]

הערכת איומים כוללת איסוף וניתוח של מודיעין על איומים פוטנציאליים באופן רציף (למשל טרור בינלאומי, איומי מדינות אויב כמו רוסיה/סין/איראן, קיצוניות פנימית וכדומה). הגופים המרכזיים הממונים על כך הם: המרכז לחקר טרור (Joint Terrorism Analysis Centre – JTAC), שהינו חלק מה-MI5 ומספק הערכות טרור מכל המקורות וקובע את רמות האיום, וצוות משותף להערכת איומים (Joint State Threats Assessment Team – JSTAT) המתמקד באיומי ביטחון לאומי.[23]

---

20 Julian Lewis (Annual Report 2021–2022). 2022. "Intelligence and Security Committee of Parliament". December 13, https://isc.independent.gov.uk/wp-content/uploads/2022/12/ISC-Annual-Report-2021%E2%80%932022.pdf

21 Julian Lewis (Annual Report 2021–2022). 2022. "Intelligence and Security Committee of Parliament". December 13, https://isc.independent.gov.uk/wp-content/uploads/2022/12/ISC-Annual-Report-2021%E2%80%932022.pdf

22 MI5 Official Website (MI5 Official Website). n.d. "The People of MI5". Accessed May 12, 2026, https://www.mi5.gov.uk/about-us

23 MI5 Official Website (MI5 Official Website). n.d. "Countering Terrorism". Accessed May 12, 2026, https://www.mi5.gov.uk/what-we-do/countering-terrorism

הדרישות נקבעות על סמך איומים, פערים וסדרי עדיפויות של משרדי ממשל קיימים. מכך נגזר מאמץ האיסוף הכולל פריסת משאבים (איסוף מודיעין ממשאבים אנושיים/CHIS, מעקב, אמצעים טכניים וכדומה). השלב הבא נוגע לפיתוח של תהליכי עיבוד וניתוח: בניית מערך מידע על איומים, גורמים עוינים, כוונות ויכולות. הערכות מותאמות באופן דינמי.[24] תהליך ההפצה כולל שיתוף עם שירותי ביטחון וסוכנויות חופפים (משטרה, SIS/MI6, GCHQ, משרדי ממשלה) לצורך מניעה או קביעת מדיניות להתמודדות. אם האיום מצדיק ודורש חקר או בירור נוספים, מוקצים לכך משאבים. החלטות לגבי היקף האיום ואופן התגובה דורשים אישור שר הפנים, והם כפופים לפיקוח ועדה פרלמנטרית.[25]

תהליך התכנון של ה-MI5 כולל פיתוח תוכניות בניין כוח, בכלל אלה תפיסת כוח אדם ופיתוח יכולות, יחד עם ניתוח תקציבים בהתאם לתפיסת הביטחון. הם עוסקים במשאבים, טכנולוגיה, שותפויות והסתגלות לאיומים מתפתחים (למשל סייבר, פעילות של מדינות עוינות, שיתוף פעולה עם מדינות חברות). הביצועים נבדקים על ידי ועדת הביטחון הלאומי של הווייטהול (Whitehall[26]).

בשנים האחרונות עבר ה-MI5 מודרניזציה והתרחבות לתחום לוחמה בטרור ואיומי פנים על הממלכה. זאת תוך שילוב משטרתי רחב יותר, למשל באמצעות יצירת קבוצות לשיתוף מודיעין, חיזוי ארוך טווח וטכנולוגיה.[27]

ה-MI5 מעסיק כ-5,000 איש.[28] מערך הגיוס כולל תהליך קפדני, תוך דגש על בדיקות סיווג ביטחוני, יכולות (למשל עבודת צוות, מקצועיות, חדשנות ויצירתיות) והתאמה לעבודה בתחומים רגישים.[29] התפקידים כוללים קציני מודיעין, חוקרים, קציני מעקב, אנליסטים, מומחים טכניים, בלשנים, מנתחים, ועובדי מנהלה (משאבי אנוש, כספים, משפט); פיתוח תוכניות לתואר שני (למשל תוכנית פיתוח לקציני מודיעין) עם כניסה ישירה לתפקיד על מגוון הרקעים.[30]

התכנון ארוך הטווח של ה-MI5 מונע על ידי איומים, מודיעין ומותאם לממשלה באמצעות הערכה מתמשכת והמחזור המודיעיני. "בניית בניין-כוח" מדגישה את החשיבות בכוח אדם מיומן, הכשרה מקצועית, יכולות טכנולוגיות ושיתופי פעולה חזקים במקום התרחבות בסגנון צבאי מסורתי. אלמנטים מסווגים מפורטים כגון הקצאת משאבים ספציפית, שיטות מבצעיות ותקציבים מדויקים אינם פומביים, מה שמגביל את דיוק ההערכות.

3.2 BfV – גרמניה

ה-Bundesamt für Verfassungsschutz (BfV, המשרד הפדרלי להגנת החוקה) הוא סוכנות הביון הפנימית הפדרלית של גרמניה, המתמקדת באיסוף מודיעין מונע כדי להגן על הסדר הדמוקרטי החופשי.

---

24 MI5 Official Website (MI5 Official Website). n.d. "Gathering Intelligence". Accessed May 12, 2026, https://www.mi5.gov.uk/how-we-work/gathering-intelligence

25 R. B. Haldane (Baidu). n.d. "MI5 British Intelligence Agency". Accessed May 12, 2026, https://baike.baidu.com/en/item/MI5/1530773

26 GlobalSecurity.org (GlobalSecurity.Org). n.d. "Organization - Security Service MI5". Accessed May 12, 2026, https://www.globalsecurity.org/intell/world/uk/mi5-org.htm. Also in Lord Beamish PC (Annual Report 2023–2025). 2025. "Intelligence and Security Committee of Parliament". December 15, https://isc.independent.gov.uk/wp-content/uploads/2025/12/ISC-Annual-Report-2023%E2%80%932025-Web-Accessible.pdf

27 MI5 Official Website (MI5 Official Website). 2015. "A Modern MI5". October 28, https://www.mi5.gov.uk/news/a-modern-mi5

28 Special Forces TV. 2026. "MI5 Explained in 4 Minutes". In YouTube. Preprint, Special Forces TV, February 6, https://youtu.be/fYdG4AGgvkI

29 Sakshi Srivastava, and Nathan Andrew (GFJob Assessment Experts). 2026. "MI5 Recruitment Process, Online Assessments, Interviews, and Assessment Centre Full Practice Guide 2026", https://www.graduatesfirst.com/mi5-assessment-tests

30 TargetJobs (TargetJobs). 2023. "Psst! The Secrets of Getting a Graduate Job with MI5, MI6 or GCHQ". January 25, https://targetjobs.co.uk/careers-advice/public-services-and-administration/psst-secrets-getting-graduate-job-mi5-mi6-or-gchq

הוא אינו גוף אכיפת חוק או גוף צבאי למחצה, אלא אוסף ומנתח מידע על איומים רלוונטיים לחוקה של הפדרציה הגרמנית, איומים כגון קיצוניות, טרור, ריגול, חבלה ואיומים נלווים.[31]

עבודתו מוסדרת על ידי BVerfSchG (חוק BfV), עם פיקוח משפטי ופרלמנטרי קפדני. תהליכי בניין כוח בהקשר זה מתייחסים לגיוס כוח אדם, הכשרה, פיתוח ארגוני ושיפור יכולות (למשל יכולות סייבר, קידום ויישום פתרונות טכנולוגיים, ניתוח מודיעין ותמיכה מבצעית).[32]

הערכת איומים וניתוח מצב מתקיימים דרך אנליסטים המעריכים מודיעין (מקורות גלויים, מקורות אנושיים ואמצעים טכנולוגיים) כדי לייצר דוחות מצב ותחזיות לגבי מגמות ארוכות טווח. התהליך מקבע סדרי עדיפויות בכמה תחומים עיקריים (למשל ימין/שמאל קיצוני, אסלאם רדיקלי, ריגול/מודיעין נגדי, הגנה קיברנטית, הגנה כלכלית/מדעית, פעולות מנע נגד ריגול תעשייתי ועוד). הערכות מנע מתרכזות סביב איסוף מידע מרבי רלוונטי באמצעות "קטלוג של דרישות מידע".[33]

תיאום וקביעת סדרי עדיפויות מתרכזים סביב תכנון הכולל את משרד הפנים הפדרלי (BMI), מרכזי שליטה ובקרה משותפים (למשל GTAZ ללוחמה בטרור) ושותפויות בינלאומיות. יחידות ניתוח ומחקר מיוחדות כמו Zentrum für Analyse und Forschung (ZAF) תומכות במחקר ופיתוח של השירות.[34]

תכנון משאבים ויכולות נמצא בסמכות של מחלקה Z (שירותים מרכזיים), המטפלת בפיתוח משאבי אנוש, תכנון תקציב ואופטימיזציה ארגונית. זה כולל ניתוח זרימת עבודה, זיהוי פערים במיומנויות (למשל סייבר, שפות, ניתוח נתונים) והתאמה למחזורי תקציב פדרליים. התקציבים חסויים, אך מאושרים על ידי ועדת התקציב של הבונדסטאג (ועדה חסויה לשירותי מודיעין).[35]

התאמה לאתגרים ורפורמות ב-BfV באות לידי ביטוי בהתאמה של המבנה והשיטות לאיומים מתפתחים (למשל דיגיטליזציה וסייבר, לוחמה היברידית, צורות קיצוניות של איומים חדשים כגון ימין, שמאל, אסלאם). דוגמאות היסטוריות של רפורמות חוצות ארגון כוללות שינויים לאחר איחוד גרמניה בשנות ה-80, שינויים לאחר פיגועי ה-11 בספטמבר ותגובות לסיכוני סייבר או התערבות זרה גוברת כגון מצד סין ורוסיה. שינויים ארגוניים (למשל של יחידות סייבר או תצפיות ויירוט ייעודיים) עוקבים אחר הצרכים המונעים על ידי איומים מתפתחים ומותאמים אליהם.[36]

הפיקוח ההדוק על ידי הרשויות על פעילות השירות מתבצע בדרכים מספר. התוכניות עוברות ביקורות משפטיות (למשל מידתיות, הגנת מידע, הגנת הפרט), ביקורת פרלמנטרית ופיקוח שיפוטי (למשל ועדת ה-G10 למעקב תקשורת וחופש ביטוי). זה מבטיח שתפיסות הפעולה תישארנה תואמות את שלטון החוק.[37]

---

31 BfV Official Website (BfV Official Website). n.d. "Mis¬sion and Work¬ing Meth¬ods". Accessed May 12, 2026, https://www.verfassungsschutz.de/EN/about-us/mission-and-working-methods/mission-and-working-methods_node.html

32 BfV Official Website (BfV Official Website). n.d. "Departments Fulfilling Specialized Tasks". Accessed May 12, 2026, https://www.verfassungsschutz.de/EN/about-us/bundesamt-fuer-verfassungsschutz/organisation/organisation_article.html

33 BfV Official Website (BfV Official Website). n.d. "Analysis and Reporting". Accessed May 12, 2026, https://www.verfassungsschutz.de/EN/about-us/mission-and-working-methods/analysis-and-reporting/analysis-and-reporting_node.html

34 UN Council. n.d. *Implementing the UN Global Counter-Terrorism Strategy*. Accessed May 12, 2026, https://www.un.org/counterterrorism/sites/default/files/2026-03/germany_-_contribution_to_sg_report_on_activities_of_the_united_nations_system_in_implementing_the_united_nations_global_counter-terrorism_strategy_2025.pdf

35 BfV Official Website (BfV Official Website). n.d. "Supervision and Oversight". Accessed May 12, 2026, https://www.verfassungsschutz.de/EN/about-us/mission-and-working-methods/supervision-and-oversight/supervision-and-oversight_node.html

36 Alexander Dobrindt. 2025. *BfV Celebrates 75 Years*. Berlin, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/allgemein/2025-10-jubilaeumsbroschuere-75-jahre-bfv.pdf?__blob=publicationFile&v=8

37 BfV Official Website (BfV Official Website). n.d. "Supervision and Oversight". Accessed May 13, 2026, https://www.verfassungsschutz.de/EN/about-us/mission-and-working-methods/supervision-and-oversight/supervision-and-oversight_node.html

תהליך בניין-הכוח של ה-BfV הוא מחזורי, וכולל את השלבים הבאים: איומים ← ניתוח ← סדרי עדיפויות באיסוף ← התאמות יכולות ← דיווח ומשוב.

בהקשר של הכשרת כוח האדם, ה-BfV גדל במידה ניכרת בתגובה לאיומים הגוברים. הגיוס לשירות כולל בדיקות ביטחוניות קפדניות וממושכות, והתמקדות בתפקידים מגוונים (כגון אנליסטים, בלשנים, מומחי IT, קציני תפעול וכו׳). מחלקה ה-Z מנהלת גיוס, שירותי משאבי אנוש, הכשרה ופיתוח.[38]

התכנון הרב-שנתי של ה-BfV הוא מחזור מתמשך, מונע על ידי ומתרכז סביב מודיעין, המעוגן בניתוח איומים ובמנדטים משפטיים פדרליים, בעוד שבניין הכוח מתמקד בגיוס ממוקד, הכשרה מיוחדת וזריזות ארגונית כדי להתמודד עם סיכונים דינמיים כמו קיצוניות, ריגול ואיומי סייבר.

הפיתוח של השירות הינו דרך תכנון משאבי אנוש הקשור לצרכים ארוכי טווח (למשל כישרונות סייבר, מדעני נתונים, מחקר ועוד). התהליך כולל שימור כוח אדם, לימודים נוספים וניידות פנימית. גידול בתקציב תומך בפיתוח של יותר משרות. בנייה ארגונית וטכנית באה לידי ביטוי בהתאמות מבניות, כגון מחלקות להגנת סייבר, הגנה כלכלית וכדומה, המשקפות סדרי עדיפויות מתפתחים; יחידות ייעודיות לתצפית (מחלקה O) ואמצעים טכניים (מחלקה 3, מחלקה T[39]).

השירות ממומן באמצעות תקציב פדרלי. התקצוב תומך ומשקיע בין השאר במודרניזציה של תחום ה-IT, מתקנים חדשים וכלים מתקדמים.[40] עיקר ההשקעות של השירות הוא בתקשורת מאובטחת, ניתוח נתונים וטכנולוגיה תפעולית, שיפור יכולות בסייבר, מודיעין קוד פתוח, קישור ושיתוף פעולה בינלאומי ושירותי התרעה לעסקים ולמוסדות מדע. שיתוף פעולה עם מדינות ובעלות ברית מגביר במידה רבה את טווח ההישגים ללא צמיחה פנימית פרופורציונלית.[41]

לסיכום, התכנון הרב-שנתי של ה-BfV הוא מחזור מתמשך, מונע על ידי ומתרכז סביב מודיעין, המעוגן בניתוח איומים ובמנדטים משפטיים פדרליים, בעוד שבניין הכוח מתמקד בגיוס ממוקד, הכשרה מיוחדת וזריזות ארגונית כדי להתמודד עם סיכונים דינמיים כמו קיצוניות, ריגול ואיומי סייבר.

3.3 FSB – רוסיה

שירות הביטחון הפדרלי הרוסי (FSB, או Federal′naya Sluzhba Bezopasnosti) הוא סוכנות הביטחון הפנימי והמודיעין הנגדי העיקרית של הפדרציה הרוסיה, היורשת העיקרית של הפונקציות הפנימיות של הקג״ב (KGB) הסובייטי. השירות עוסק בעיקר במודיעין נגדי, לוחמה בטרור, אבטחת גבולות (דרך שירות הגבולות שכפוף לו), ביטחון כלכלי, הגנה על הסדר החוקתי, אבטחת מידע/סייבר ותיאום מאמצי המודיעין הנגדי של סוכנויות אחרות.[42]

---

38 Lars Oliver Michaelis. 2000. “Political Parties under the Observation of the Federal Office for the Protection of the Constitution – Militant Democracy between Tolerance and Readiness to Defend”. Baden-Baden

39 BfV Official Website (BfV Official Website). n.d. “The Ger¬man Do¬mes¬tic In¬tel¬li¬gence Ser¬vices”. Accessed May 12, 2026, https://www.verfassungsschutz.de/EN/home/home_node.html

40 Lars Oliver Michaelis. 2000. “Political Parties under the Observation of the Federal Office for the Protection of the Constitution – Militant Democracy between Tolerance and Readiness to Defend”. Baden-Baden.

41 BfV Official Website (BfV Official Website). n.d. “The Ger¬man Do¬mes¬tic In¬tel¬li¬gence Ser¬vices”. Accessed May 12, 2026, https://www.verfassungsschutz.de/EN/home/home_node.html

42 International Business Relations Corporation. 2002. *Status of the State Licensing System of Control over Exports of Nuclear Materials, Dual-use Commodities and Technologies in Russia: Manual for foreign associates in Russia*. Moscow.

מידע גלוי מפורט על התכנון ארוך הטווח הפנימי שלו ובניית בניין-כוח (כולל גיוס והכשרת כוח אדם, מימון, מבנה ופיתוח יכולות) מוגבל בשל אופיו החסוי. מידע רב מגיע מפרסומים רוסיים רשמיים, חוקים, עריקים ועיתונות חוקרת. ה-FSB פועל כגוף מבצע פדרלי הכפוף ישירות לנשיא רוסיה, עם אוטונומיה והשפעה משמעותיות חוצות משרדים, תחומים, מוסדות וארגונים.[43] נשיא רוסיה הנוכחי, ולדימיר פוטין, היה ראש השירות עד שנת 1999 לפני עלייתו לשלטון, מכך נובע לרוב כוחו הכמעט בלתי מוגבל של שירות ה-FSB בגבולות הפדרציה הרוסית.

ה-FSB מסתנכרן עם מערכת התכנון הרב-שנתית הרחבה יותר של רוסיה, הנשלטת על ידי החוק הפדרלי משנת 2014 "לתכנון אסטרטגי בפדרציה הרוסית". זה כולל את תפיסת הביטחון הלאומי של רוסיה, דוקטרינות ותחזיות המתואמות ברמות הגבוהות ביותר, ולעיתים קרובות מעורבות במועצת הביטחון של הפרלמנט הרוסי (שם ראשי ה-FSB לשעבר, כמו למשל ניקולאי פטרושב, היו בעלי השפעה פוליטית רבה).[44]

אלמנטים רלוונטיים מרכזיים בתוך ה-FSB כוללים מחלקה ייעודית לניתוח, חיזוי ותכנון רב-שנתי (חלק משירות המידע המבצעי והיחסים הבינלאומיים, יורשתם של אלמנטים מהאגף ה-5 של הק.ג.ב.). יחידה זו מבצעת הערכת איומים, תכנון תרחישים, חיזוי לטווח ארוך, ומפתחת דוקטרינות מבצעיות. היא מנתחת איומים פנימיים (טרור, קיצוניות, בדלנות, השפעה זרה), סיכונים חברתיים-כלכליים ונושאים של "החו"ל הקרוב" (מדינות סובייטיות לשעבר).[45]

התכנון מדגיש איומים היברידיים, אי-יציבות פנימית ולוחמת מידע. הוא כולל מטרות לטווח קצר, בינוני וארוך, הערכת סיכונים ותיאום בין-סוכנותי (למשל עם הגוורדיה הלאומית — Rosgvardiya, ה-SVR — שירות מודיעין חוץ, וה-GRU — מודיעין צבאי).[46]

תהליך בניין הכוח מתבצע מלמעלה למטה, מנוהל על ידי ראש ה-FSB (כיום אלכסנדר בורטניקוב) וסגניו, ובסופו של דבר מאושר על ידי הנשיא. התהליך כולל תשומות ממנהלות אזוריות, שירותים מיוחדים (למשל מודיעין נגדי, ביטחון כלכלי), מוסדות אקדמיים ומרכזי הכשרה. התהליך הוא איטרטיבי, מתמשך ומשלב לקחים מפעולות עבר (למשל פעילויות הקשורות לשתי מערכות בצ'צ'ניה בין 1999—2004, פיגועי טרור גדולים כמו בני ערובה בבית ספר בעיר בסלן ב-2004 ואירוע בני ערובה בתאטרון נורד' אוסט במוסקבה ב-2002, המלחמה באוקראינה, סנקציות בינלאומיות ועוד). השירות מרבה להשתמש בתרגילי אי-ודאות לצורך בחינת העתיד, שלעיתים קרובות מתואמים עם מועצת הביטחון הרוסית.[47]

הקצאת משאבים של השירות קשורה לתקציבים פדרליים, תוכניות חימוש ממלכתיות (רכישת טכנולוגיות, ציוד, נשק חדש ועוד) ותכנון גיוס. סדרי העדיפויות כוללים יכולות סייבר, מוכנות כוחות מיוחדים וחיזוק גבולות. אופקי התכנון תואמים לדוקטרינה מדינית (למשל אסטרטגיה לשנת 2035), עם התאמות לאירועים מתפתחים כמו הפלישה לאוקראינה ב-2022[48].

---

43 Oscar Rosengren. 2026. "The FSB: Russia's Federal Security Service". April 22, https://greydynamics.com/the-fsb-russias-federal-security-service

44 Andrey Klimenko, and Alexander Kalgin. 2018. "Strategic Planning In The Russian Federal Government: Implementation, Costs, And Conditions Of Effectiveness", https://publications.hse.ru/pubs/share/direct/218036191.pdf

45 International Business Relations Corporation. 2002. *Status of the State Licensing System of Control over Exports of Nuclear Materials, Dual-use Commodities and Technologies in Russia: Manual for foreign associates in Russia*. Moscow.

46 Andrew Monaghan. 2021. "How Russia Does Foresight". *EUISS European Union Institute for Security Studies*, January 29, https://www.iss.europa.eu/publications/briefs/how-russia-does-foresight

47 Andrew Monaghan. 2021. "How Russia Does Foresight". *EUISS European Union Institute for Security Studies*, January 29, https://www.iss.europa.eu/publications/briefs/how-russia-does-foresight

48 Vladimir Putin. 2021. *About National Security Strategies*, https://rusmilsec.blog/wp-content/uploads/2021/08/nss_rf_2021_eng_.pdf

מבנה הארגון מתחיל במטה המרכזי, המוכר על פי מיקומו ברחוב לוביאנקה (מוסקבה), המפקח על שירותים ומנהלות (למשל שירות מודיעין נגדי, שירות ביטחון כלכלי, שירות להגנת הסדר החוקתי והמאבק בטרור, מידע מבצעי, יחסים בינלאומיים, שירות ארגוני וכוח אדם, שירות גבול, מרכז ייעודי עם יחידות עיליות כמו כוח מיוחד מבצעי "אלפא" ויחידת "ווימפל").[49] מנהלות אזוריות עוסקות בנושאים פדרליים; יחידות טריטוריאליות מטפלות בפעולות מקומיות. הרפורמות תחת שלטונו של ולדימיר פוטין הרחיבו את סמכויות ה-FSB, יצרו מנהלות חדשות (למשל לאבטחת סייבר/מידע) וחיזקו את השליטה על סוכנויות אחרות.[50]

יחידות מיוחדות של השירות (למשל אגף תעופה, אגף מדעני-טכני, ביטחון פנים) ומתקני הכשרה ומחקר תומכים יחד ומהווים חלק מתהליך צמיחה ופיתוח. תהליך גיוס ופיתוח מערך כוח אדם נע בעיקר סביב גיוס קציני צבא תוך איתור כוח אדם מאקדמיות צבאיות, מתחום אכיפת חוק וממוסדות אחרים, תוך דגש על אמינות אידאולוגית, פטריוטיות ומערך בידוק וסינון (בדיקות רקע, פוליגרף, נאמנות למשטר).

מחלקת ארגון וכוח האדם מנהלת את מערך הגיוס, קידומים, רוטציות וגיוס קצינים "מושאלים" מגופים אחרים (ה-FSB משתלב בגופי ממשלה אחרים לצורך השפעה פוליטית עליהם ורשאי לשאוב מועמדים ומשאבים).[51] התמריצים כוללים מעמד גבוה, שכר, הטבות וניידות חברתית. הגיוס מכוון לבוגרי אוניברסיטאות, אנשי צבא לשעבר ומומחים (למשל בתחום ה-IT/סייבר). אלמנטים כפייתיים או אופורטוניסטיים מודגשים במבצעים של הארגון (למשל גיוס סוכני השפעה, פעילים עבור מבצעי חבלה, מרגלים, מלשינים ועוד).[52] האימונים מתקיימים באקדמיות ובמרכזים של ה-FSB (למשל לסיכול מודיעין, מבצעים מיוחדים, סייבר). המיקוד כולל אומנויות מבצעיות, שפות, מיומנויות טכנולוגיות ותרגילים משותפים. יחידות עילית כמו אלפא/ווימפל מקיימות מיון קפדני ותוכניות ייעודיות ללוחמים מיחידות מיוחדות קרביות.

לאחר שנות ה-2000 בוצעו השקעות מהותיות בתחום של יחידות לפעולות התקפיות/הגנתיות, מעקב והגנה/תקיפה של תשתיות קריטיות, לוחמה אלקטרונית ועוד, כמו גם הרחבה ושיפור יכולות של כוחות מיוחדים ומשמר הגבול כולל הרחבת יחידות תגובה מהירה (טקטיות), תמיכה תעופתית וכוחות/ציוד שמירת גבולות. פיתוח טכני/מדעי מתקיים במכוני מחקר לכלי עבודה וציוד חדשים (מעקב, זיהוי פלילי, לוחמה אלקטרונית).

גיוס ורמת המוכנות מותאמים לתוכניות גיוס לאומיות כולל מילואים, מערך מצבי חירום, אסונות, אירועים רבי-נפגעים ומלחמה, והרחבת מערך מעצרים מבצעיים.[53] הבנייה היא הדרגתית, מונעת על ידי שיקולי תקציב ומגיבה בראש ובראשונה לאיומים קבועים (נאט"ו, אי-יציבות פנימית, טרור). היא נותנת עדיפות לאיכות בצוותים ותפקידים מרכזיים תוך תחרות על כישרונות עם המגזר הפרטי (בייחוד בסייבר).

---

49 Oscar Rosengren. 2026. "The FSB: Russia's Federal Security Service". April 22, https://greydynamics.com/the-fsb-russias-federal-security-service. Also in International Business Relations Corporation. 2002. *Status of the State Licensing System of Control over Exports of Nuclear Materials, Dual-use Commodities and Technologies in Russia: Manual for foreign associates in Russia.* Moscow.

50 Oscar Rosengren. 2026. "The FSB: Russia's Federal Security Service". April 22, https://greydynamics.com/the-fsb-russias-federal-security-service

51 Oscar Rosengren. 2026. "The FSB: Russia's Federal Security Service". April 22, https://greydynamics.com/the-fsb-russias-federal-security-service

52 The Moscow Times. 2025. *FSB Recruits Ukrainian Teenagers for Espionage and Sabotage – FT*. June 30, https://www.themoscowtimes.com/2025/06/30/fsb-recruits-ukrainian-teenagers-for-espionage-and-sabotage-ft-a89617/pdf

53 International Business Relations Corporation. 2002. *Status of the State Licensing System of Control over Exports of Nuclear Materials, Dual-use Commodities and Technologies in Russia: Manual for foreign associates in Russia*. Moscow.

לסיכום, התכנון הרב-שנתי של ה-FSB הוא תהליך מובנה, המוטמע בארכיטקטורת הביטחון הלאומי של רוסיה, תוך דגש על נטרול איומים פרואקטיבי. בניית הכוח מתמקדת בהתמקצעות, ביתרון טכנולוגי (בייחוד בסייבר), בחיזוק יחידות עיליות ובקידום השפעה פולשנית.

3.4 FBI – ארצות הברית

התכנון לבניין-הכוח של ה-FBI וגיוס סוכנים לשירות הם תהליכים קשורים זה לזה המשלבים משאבים, כוח אדם ופעולות עם התמודדות מול איומים לאומיים מתפתחים כמו טרור, איומי סייבר, מודיעין נגדי, פשיעה אלימה ושחיתות ציבורית. אלה מעוצבים על ידי משימתו של ה-FBI להגן על העם האמריקאי ולהבטיח קיום החוקה, עם חזון "להיות לפני האיום" (ahead of the threat) באמצעות מנהיגות, זריזות ואינטגרציה.[54]

תהליך התכנון לבניין כוח של ה-FBI מיושם על ידי שימוש במסגרת תכנון מובנית המשלבת הערכת איומים, קביעת סדרי עדיפויות, הקצאת משאבים והערכת ביצועים. התכנון שואב מניסיון ניהולי וביצועי פדרליים, כמו חוק ביצוע ותוצאות הממשלה (Government Performance and Results Act), וכלים למעקב, דוגמת המעקב אחר ביצוע מאוזן (Balanced Scorecard).[55]

חטיבות המבצעים של המטה מנתחות מודיעין ואיומים במערך חוצה ארגון. הן קובעות את סדרי העדיפויות הלאומיים של ה-FBI (למשל לוחמה בטרור כעדיפות עליונה לאחר ה-11 בספטמבר, לצד איומים בסייבר, מודיעין נגדי ופלילים). זה כולל הערכת איומים מקומית, ניתוח ותיאום עם שותפים בקהיליית המודיעין, משרד ביטחון הפנים האמריקאי (DHS) ואכיפת החוק הכלל-מדינתית (פדרלית) והמקומית בכל מדינה.[56]

משרדי שטח (56) ומשרדי התובעים המקומיים מפתחים תוכניות מקומיות המותאמות לאיומים אזוריים.[57] התוכניות משלבות אלמנטים כמו ניתוח רציונל (כדאיות משאבית וביטחונית), ניתוחי SWOT, פערים, מטרות, יעדים ומדדי ביצוע.[58] להבדיל מסוכנויות ביטחון פנים אחרות, הכפופות לרוב למשרד הפנים או כגוף נפרד הכפוף לממשל, ה-FBI בהיותו גוף חקירות משפטי כפוף למשרד המשפטים האמריקאי – United States Department of Justice (DOJ) . הערכות אמצע שנה וסוף שנה מעריכות את ההתקדמות מול היעדים. מונפקים סקירות ודו"חות שוטפים על ידי מנהלים, ראשי אגפים, מנהלי שטח ומנהלי תוכניות (פרויקטים) העוקבים אחר האפקטיביות וביצועי הארגון.[59]

אגף התכנון מעביר ישירות לאגף התקצוב את בקשת התקציב השנתית וזו מועברת לקונגרס דרך משרד המשפטים. בקשות התקצוב כוללות התאמות ליעדי השירות השוטפים ושינויים בתוכניות (למשל שיפורים בתחום הסייבר, לוחמה בטרור או פשיעה אלימה). תכנון רב-שנתי פרוס על גבי יוזמות ופרויקטים ייעודיים. תקציבים מתפרסים ליחידות קבלת החלטות: ביטחון לאומי, מודיעין, אכיפת חוק ומשפט פלילי.[60]

---

54 FBI Official Website. 2023. *Federal Bureau of Investigation (FBI) 2023 Budget Report*, https://www.justice.gov/jmd/page/file/1489476/dl

55 Bernard Marr. 2015. "How the FBI Manages Performance". In *LinkedIn*. Preprint, January 26, https://www.linkedin.com/pulse/how-fbi-manages-performance-bernard-marr

56 *FBI 2023 Budget Report*, https://www.justice.gov/jmd/page/file/1489476/dl

57 Ibid.

58 Cris Hoover (FBI Articles). 2010. "The Strategic Communication Plan". August 1, https://leb.fbi.gov/articles/featured-articles/the-strategic-communication-plan

59 *FBI 2023 Budget Report*, https://www.justice.gov/jmd/page/file/1489476/dl

60 Ibid.

תכנון בניין כוח אדם עוסק בגיוס, הכשרה ושימור. משרד תכנון המשאבים (Resource Planning Office RPO) במטה ממלא תפקיד מרכזי בניהול תקציב כוח אדם, תכנון כוח אדם, מדיניות ושימוש בכלים של תכנון ומודיעין מהעולם העסקי (business intelligence tools[61]).

גישת ה-FBI היא פרואקטיבית ואיטרטיבית, ומאזנת גישה מרכזית עם ביצוע מבוזר. תוכניות מפורטות עדכניות או אלמנטים מסווגים אינם פומביים במלואם, אך הצדקות תקציביות לא מסווגות ועדויות רשמיות מספקות שקיפות רבה יחסית בנתונים.

התכנון של גיוס והכשרה של כוח אדם משולב עם תכנון רב-שנתי והערכת יכולות כוח האדם הנוכחי מול צרכים מצופים עתידיים (למשל מיומנויות סייבר, אנליסטים מודיעיניים, מומחי שפות ועוד). בנוסף, מתקיים זיהוי פערים במיומנויות או פיזור כוח אדם (למשל העברת סוכנים למשרדי שטח או פרויקטים עם עדיפות). השיקולים העיקריים נעים סביב סדרי עדיפויות לאיומים, תקציב, נשירה וגלי פרישה.[62]

בנוסף ישנן דרישות ובקשות כוח אדם מונחות תקציב. הגשות תקציב שנתיות מבקשות הגדלת תפקידים ספציפיים (למשל מאות סוכנים מיוחדים, מומחים למידע וצוות תמיכה לסייבר או ללוחמה בטרור). כמו כן קיימת רוטציה (מחזוריות) בהקצאות כוח אדם (למשל העברת תפקידים מהמטה למשרדי שטח).[63]

התמקדות במיומנויות כמו ניתוח נתונים, אבטחת סייבר וגיוון ההתמחות. אתגרים מרכזיים והתאמות טמונים בטרנספורמציה שלאחר ה-11 בספטמבר: מעבר מאכיפת חוק תגובתית לפעולות מנע מבוססות מודיעין, עם הקצאת סמכויות משמעותית של סוכנים ל-CT/CI. התאמה לאיומים מתפתחים עם התמקדות מוגברת בתחום הסייבר, הקצנה בתוך ארה"ב (domestic radicalization) והשפעה זרה דורשים שינויים בגיוס והכשרה מיוחדת המותאמת לאיומים מתפתחים חדשים.

גישת ה-FBI היא פרואקטיבית ואיטרטיבית, ומאזנת גישה מרכזית עם ביצוע מבוזר. תוכניות מפורטות עדכניות או אלמנטים מסווגים (למשל סדרי עדיפויות ספציפיים לאיומים) אינם פומביים במלואם, אך הצדקות תקציביות לא מסווגות ועדויות רשמיות מספקות שקיפות רבה יחסית בנתונים.

4 בינה מלאכותית בתכנון בניין כוח

בינה מלאכותית משולבת יותר ויותר בתכנון רב-שנתי, הערכת סיכונים, הקצאת משאבים, פיתוח כוח אדם ובניית יכולות תפעוליות בסוכנויות ביטחון פנים של ארה"ב, ובייחוד במשרד לביטחון פנים של ארה"ב (DHS) ובמרכיביו. המשרד לביטחון פנים פרסם תפיסה ייעודית של בינה מלאכותית, מפות דרכים ורשימות של מקרי שימוש המנחות אימוץ אחראי, תוך התמקדות בשיפור משימות, הפחתת סיכונים והרחבת יכולות. [64]

61 FBI Resource Planning Office. n.d. *Federal Bureau of Investigation*. Accessed May 13, 2026, https://www.umw.edu/careercenter/wp-content/uploads/sites/41/2020/09/RPO_One_Pager_New_Version.pdf
62 GAO United States General Accounting Office. 2004. *FBI Transformation: FBI Continues to Make Progress in Its Efforts to Transform and Address Priorities*, https://www.gao.gov/assets/a110739.html
63 FBI Federal Bureau of Investigation. 2027. FY 2027 *FBI Budget Request to Congress*, https://www.justice.gov/jmd/media/1434246/dl?inline
64 Markwayne Mullin (DHS US Department of Homeland Security). 2026. "DHS Delivers on White House's Commitment to AI Innovation, Governance, and Public Trust", https://www.dhs.gov/ai

תפיסת הבינה המלאכותית של ה-DHS (בהתאם ל-OMB M-25-21) מתמקדת בהסרת חסמים לשימוש אחראי בבינה מלאכותית, שיפור וקידום השימוש בבינה המלאכותית ברחבי המשרד, והבטחת שקיפות ואחריות. היא כוללת יעדים של שילוב בינה מלכותית בתשתיות של הארגון וביצוע משימות בסיוע בינה מלאכותית. סדרי העדיפויות כוללים שדרוג מיומנויות כוח אדם, הרחבת מו"פ, מעקב/תכנון משאבים להשקעות עתידיות בבינה מלאכותית, וקשירת יוזמות בינה מלאכותית לתוצאות הניתנות למדידות.[65]

סוכנויות משתמשות בבינה מלאכותית לצורך מיזוג מודיעין, אופטימיזציה לוגיסטית, ניהול שרשרת אספקה במצבי חירום ויישומים הגנתיים (למשל הנדסה הפוכה של תוכנות זדוניות וזיהוי אנומליות ברשת). מסגרות עבודה מתייחסות לסיכוני בינה מלאכותית לתשתיות קריטיות, ומקדמות אימוץ אחראי תוך הגנה מפני שימוש עוין בבינה מלאכותית.[66] מאמצים אלה מדגישים את הגישה של "האדם בתוך התהליך" (human-in-the-loop), מפיילוטים ועד לשימוש ארגוני מלא.[67]

4.1 סריקת האופק

סריקת האופק (Horizon Scanning) בשילוב בינה מלאכותית היא מתודולוגיה מתקדמת לאיתור מוקדם של מגמות, טכנולוגיות מתפתחות, סיכונים והזדמנויות שצפויות להשפיע על ארגונים, תעשיות ומדינות.[68] המתודולוגיה משלבת גישות מסורתיות של סריקה שיטתית עם יכולות חישוביות עוצמתיות של בינה מלאכותית, מה שהופך את התהליך למהיר, מקיף ומדויק בהרבה בהשוואה לשיטות ידניות. התהליך כולל כמה שלבים:

הגדרת היקף – שלב זה מהווה את הבסיס לכל התהליך ומבטיח שהסריקה ממוקדת. בשלב זה מגדירים בבירור את **הנושא**, התחומים הרלוונטיים, אופק הזמן (למשל 3–5 שנים, 10 שנים או יותר), והמטרות ארוכות הטווח (זיהוי סיכונים, הזדמנויות, מגמות טכנולוגיות וכדומה). בשילוב בינה מלאכותית יוצרים מפות נושאים ראשוניות או ניתוח סמנטי של שאילתות כדי להגדיר מילות מפתח וגבולות. השלב כולל גם זיהוי בעלי עניין (Stakeholders) והגדרת קריטריונים להערכת חשיבות. ללא הגדרה מדויקת, הסריקה עלולה להיות רחבה מדי או צרה מדי.

איסוף – זהו שלב האיסוף השיטתי של כמויות גדולות של מידע. באמצעות בינה מלאכותית, הכלי סורק אוטומטית אלפי מקורות: מאמרים מדעיים (Scopus, PubMed), דוחות, רשתות חברתיות, RSS feeds, API ועוד. ה-AI מנקה נתונים (de-duplication), מתרגם שפות ומסמן מטא-נתונים ראשוניים.

זיהוי אותות חלשים (Weak Signals Identification) – זהו שלב קריטי המתמקד בזיהוי "אותות חלשים" – סימנים ראשוניים, לא בולטים, לשינויים עתידיים, לצד מגמות (Trends) ואירועים פוטנציאליים (Wild Cards). הבינה המלאכותית משתמשת במודלים של למידה עמוקה כדי לזהות דפוסים נסתרים, קשרים בין-תחומיים ועלייה חדה בדיונים.

---

65 Antoine McCord. 2025. Department of Homeland Security Artificial Intelligence (AI) Strategy, https://www.dhs.gov/sites/default/files/2025-09/25_0926_cio_dhs_ai_strategy_for_omb_m-25-21_508.pdf

66 DHS Official Website (DHS US Department of Homeland Security). n.d. "Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure". Accessed May 15, 2026, https://www.dhs.gov/publication/roles-and-responsibilities-framework-artificial-intelligence-critical-infrastructure

67 NGA Center for Best Practices, National Governors Association. 2018. *Leveraging AI for Homeland Security and Emergency Management*, https://www.nga.org/wp-content/uploads/2019/08/AI-in-Homeland-Security-and-Emergency-Management-Memo.pdf

68 Building capacity in technology horizon scanning: A guide for policymakers, OECD Science, Technology and Industry Working Papers, 06.2026, https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/04/building-capacity-in-technology-horizon-scanning_7a0a98c6/b4f0d383-en.pdf

ניתוח והערכה (Analysis & Evaluation) – בשלב זה הופכים את הנתונים הגולמיים לתובנות. ה-AI מבצע ניתוח סנטימנט, חיזוי התפתחויות, יצירת Knowledge Graphs (גרפים של קשרים) וסימולציות של תרחישים (Scenarios) באמצעות Generative AI. מודלים ייעודיים מנתחים קשרים, מעריכים השפעה וסבירות, ומזהים דפוסים בין-תחומיים. השלב כולל גם שימוש במומחים אנושיים הבודקים ומשפרים את התוצאות של ה-AI כדי להפחית הטיות ולשפר דיוק.

סינון, ויזואליזציה והמלצות (Filtering, Visualization & Recommendations) – השלב האחרון הופך את הניתוח לפעולה מעשית. ה-AI מסנן אותות לפי רלוונטיות ועוצמה, מייצר המחשה (גרפים תלת-ממדיים, מפות חום, Knowledge Graphs אינטראקטיביים) ומפיק דוחות, תרחישים והמלצות. בסופו של דבר, קבלת החלטות על בסיס התובנות.

שילוב בינה מלאכותית מאפשר עיבוד נתונים בזמן אמת, זיהוי דפוסים נסתרים והפחתה משמעותית של הטיות אנושיות, תוך שמירה על האדם כגורם מפרש ומקבל החלטות. דוגמאות מעשיות כוללות את כלי ה-UN Global Horizon Scanning, מערכות כמו Athena של Shaping Tomorrow (שסורקת עשרות אלפי מקורות), וכלים פתוחים כמו SCANAR ו-AIDOC. בישראל, משרד המדע מפעיל מעבדה לסריקת אופק מבוססת בינה מלאכותית, כולל מערכות Multi-Agent, לצורך מתן התראות למקבלי החלטות.[69]

4.2 ניתוח חיזוי

ניתוח חיזוי (Predictive Analytics) והערכת סיכונים בראייה ארוכת טווח הינו מרכיב בתהליך תכנון לבניין כוח. הסוכנות הפדרלית למקרי חירום (FEMA) משתמשת בבינה מלאכותית למידול פריסת כוח אדם לניהול אירועים (ניבוי צורכי משאבים על סמך נתוני אסונות היסטוריים) ותכנון הפחתת סיכונים (GenAI מסייע ביצירת סעיפי תוכנית תואמי רגולציה עבור רשויות מקומיות, משפר את הזכאות למענקים ואת החוסן). ראייה ממוחשבת המונעת על ידי בינה מלאכותית מעריכה נזקי אסונות מצילומי אוויר, ומאפשרת הקצאת משאבים מהירה ויעילה יותר.[70]

הרשות האמריקנית להגנה בסייבר ולהגנה על תשתיות קריטיות (CISA) משתמשת בלמידת מכונה לניתוח פגיעויות סייבר, מיון נתונים ממקורות כמו "קטלוג הפגיעויות" (Known Exploited Vulnerabilities Catalog), לקבלת היגיון תפעולי/המלצה על דרכי פעולה. תהליך זה תומך בתכנון של הגנת סייבר.[71] גם רשות המכס וההגנה על הגבולות, ה-CBP, משתמשת במודלים של למידת מכונה כדי לזהות ולנתח דפוסים היסטוריים, לסמן פעילות חשודה (למשל גילוי סמים) ולסנן מטען/תמונות צילומים בזמן אמת. בינה מלאכותית מגבירה את המודעות לפריסת משאבים בתכנון שמירת גבולות.[72]

---

69 רפאל קאהאן, לישראל יש מערכת בינה מלאכותית שמנסה לחזות את העתיד | בלעדי, YNET, 3.9.2025.

70 American University (American University. Washington DC). n.d. "The Impact of AI and Cybersecurity on Homeland Security". Accessed May 15, 2026, https://www.american.edu/online/online-program/online-master-of-science-in-counter-terrorism-and-homeland-security/the-impact-of-ai-and-cybersecurity-on-homeland-security.cfm

71 DHS US Department of Homeland Security. 2025. *Artificial Intelligence Use Case Inventory*, https://data.aclum.org/storage/2025/01/DHS_www_dhs_gov_data_AI_inventory.pdf

72 DHS Official Website (DHS US Department of Homeland Security). n.d. "DHS Delivers on White House's Commitment to AI Innovation, Governance, and Public Trust". Accessed May 15, 2026, https://www.dhs.gov/ai

5 מתודולוגיה לתכנון לבניין הכוח – מודל מוצע

מתוך הידע והניסיון של אחד מכותבי מסמך זה, מוצע להלן מודל לתהליך תכנון לבניין כוח המתאים לארגון. טרם הפירוט והדיון בנושאי תהליכי התכנון לבניין הכוח נדרש לסכם הגדרות וקביעות יסוד כדלהלן:

הפעלת הכוח למימוש הייעוד. בהקשר זה ניתן לנסח שתי קביעות כלליות: 1) מימוש ייעוד מתקיים על ידי ביצוע משימות הפעלת כוח. 2) תפוקות הפעלת הכוח מתקבלות על ידי פעולות חיצוניות.

בניין הכוח: הגדרה – בניית יכולות הפעלת הכוח. בהקשר זה ניתן לנסח שתי קביעות כלליות: 1) פעולות בניין הכוח ממומשות על ידי פעולות פנימיות. 2) התמיכה במשימות הפעלת כוח קונקרטיות אף שהיא פעילות פנימית תיחשב כחלק מהפעלת הכוח. תיאור סכמתי של הגדרות אלה ניתן לראות בתרשים להלן:

לצורך אפיון תהליכי התכנון לבניין הכוח הוגדרו הנחות היסוד הבאות: 1) כל התהליכים והפעולות באים לשרת את הפעלת הכוח. 2) מטרת בניין הכוח היא להגדיל את התפוקה המבצעית של הפעלת הכוח ולהתאימה לצרכים המשתנים. זו ניתנת למדידה על ידי התבחינים הבאים: הגדלת כמות והיקף המבצעים (משימות ופעילויות), הגדלת היכולת לבצע משימות הפעלת הכוח והקטנת היחס שבין תקורות בניין הכוח לתפוקות הפעלת הכוח.

אחד המאפיינים העיקריים של תהליכי בניין הכוח הוא טווח הזמן. אופק התכנון לתהליכי תכנון בניין הכוח יהיה שלוש שנים (עד חמש שנים במקרים מיוחדים), מהן תיגזרנה תוכניות שנתיות מפורטות. תוכניות בניין הכוח תוטמענה בתוכנית העבודה השנתית. זה יהיה הכלי לתכנון ולבקרה השנתית של כל המשימות (להפעלה ולבניין כוח).

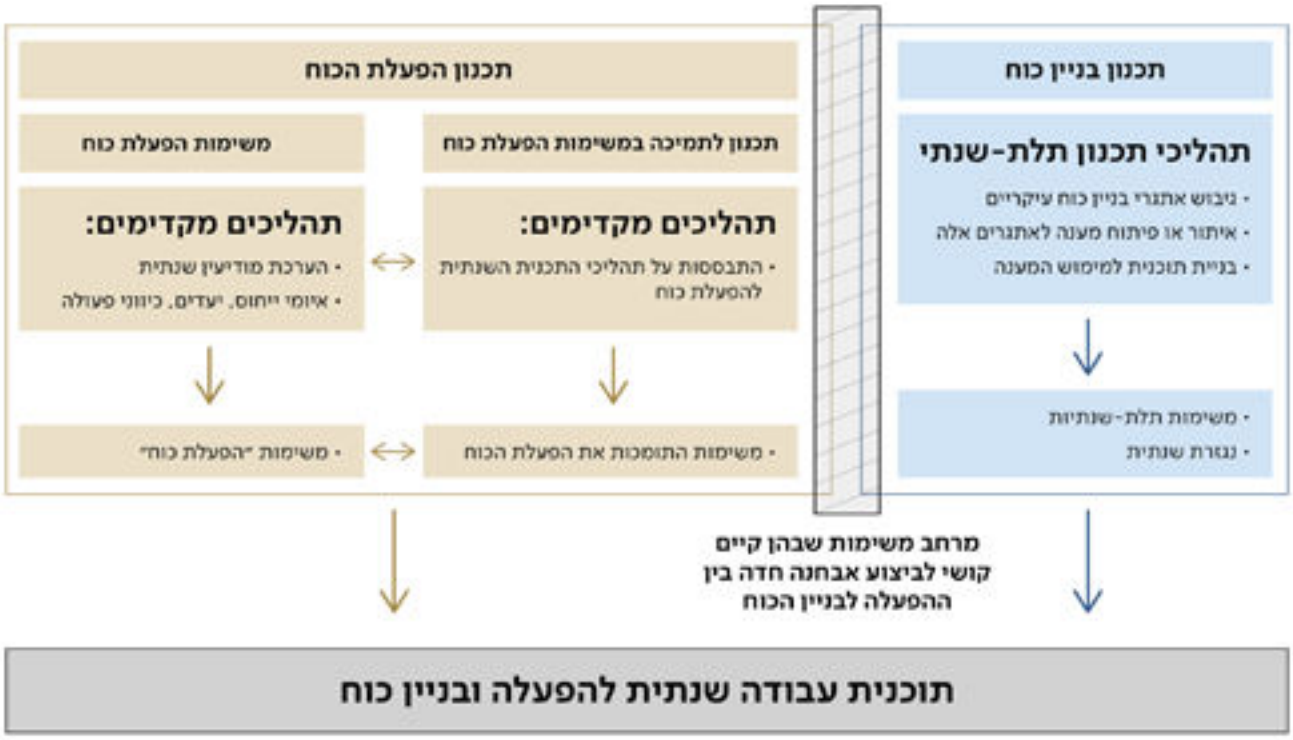
5.1 תהליך התכנון הכולל

תהליך התכנון הכולל יתבסס על שני תהליכים מקבילים:

תכנון הפעלת כוח – זהו תהליך התכנון הנוגע למשימות הפעלת הכוח למגוון הצרכים והיעדים, בכלל זה משימות הגורמים השונים הנדרשים לתמיכה בהפעלת הכוח.

תכנון לבניין כוח – זהו תהליך תכנון למימוש בניין כוח כלל-ארגוני. ככלל, למשימות אלה אין זיקה מיידית למשימות קונקרטיות. מטבע הדברים תהליכי הבנייה של יכולות ארוכות טווח יתבססו, כאמור, על תכנון תלת-שנתי אשר ממנו נגזרות משימות בניין כוח שנתיות.

פירוט זה ניתן לתיאור על ידי התרשים הבא:



5.2 תכנון בניין כוח

תכנון בניין הכוח הוא תהליך תכנון ובקרה של תהליכי הבנייה של יכולות מבצעיות חדשות, שדרוגן של יכולות קיימות ופיתוח תשתיות בתהליך תכנון תלת-שנתי אשר ממנו נגזרים פרויקטים ופעילויות בניין כוח שנתיות.

5.2.1 הערכת מצב תלת-שנתית – גיבוש אתגרי בניין הכוח

בתהליך זה ניתן לעשות שימוש במתודולוגיות סקירת האופק לעיל (בסיוע בינה מלאכותית) וכדומה. גיבוש האתגרים העיקריים לבניין כוח על ידי בחינה של כמה מרכיבים, דוגמת:

ניתוח קשת האיומים – בחינה וניתוח של מרכיבי האיום על המדינה ואפיון עיקרי היעדים הרלוונטיים בשנים הקרובות בזיקה להם.

איומים על הפעלת הכוח – ניתוח קשת האיומים על מרכיבי הפעולה.

ניתוח הסביבה הטכנולוגית – כיווני התפתחות נצפים, הזדמנויות וסיכונים טכנולוגיים.

ניתוח הסביבה הכלכלית/תקציבית – בחינה וניתוח של הסביבה הכלכלית בשנים הקרובות וניתוח סיכונים.

הסביבה החיצונית – ניתוח הסביבה הדיפלומטית ויחסי החוץ של המדינה בהקשרים רלוונטיים.

ניתוח הסביבה הפנימית – ניתוח השפעות על הפעולה כתוצאה מהסביבה הפנימית במדינה, כולל: היבטי שיתוף פעולה בין-ארגוני מול פיתוח יכולות עצמאיות.

ניתוח יכולות מבצעיות נדרשות – בחינה של היכולות המבצעיות העיקריות שתידרשנה בשנים הבאות.
ניתוח תשתיות ארגוניות – בחינה של צורכי התשתיות הארגוניות העיקריות שתידרשנה בשנים הקרובות.

5.3 גיבוש המענה לאתגרים המרכזיים

חלק זה בתהליך בוחן את התפיסה הכללית העונה לאתגרים שאופיינו. ניתן להעריך שמורכבותם של חלק מהאתגרים לא תאפשר תפיסת מענה סדורה כבר בשלב זה. לכן התוצר של שלב זה יחלק את האתגרים לשתי קבוצות:

אתגרים שיש להם תפיסת מענה מוסכמת – אתגרי בניין כוח שתפיסת המענה שלהם ברורה, מקובלת ומוסכמת. התבחין לקיומה של תפיסת מענה סדורה הוא ביכולת לפרק תפיסה זו לאבני היסוד לבניין הכוח ולייצר משימת בניין כוח מגובשת וסגורה. הקריטריון לקיומה של תפיסת מענה יכלול את המרכיבים הבאים:

- המענה מתבסס על טכנולוגיה זמינה, בדוקה ואמינה.
- המענה מתבסס על עקרונות פעולה ידועים ומזוהים הניתנים לניסוח.
- ניתן לתכנן מסגרת לבניית היכולת או למימוש פרויקט בטווח זמן רלוונטי.
- ניתן לאפיין למענה מסגרת תקציבית ברמת ודאות גבוהה הן להקמת היכולת והן לתחזוקתה לאורך שנים.

אתגרים שנדרש לפתח להם תפיסת מענה – אלו הם האתגרים שלא קיימת להם תפיסת מענה סדורה ולא ניתן לייצר להם משימת בניין כוח סגורה. לכן אתגרים אלו מחייבים תהליכי גיבוש תפיסתיים מקדימים.

5.4 קביעת מענה לאתגרים המרכזיים בבניין הכוח

כאמור, חלק מהאתגרים שלגביהם תקף הצורך באפיון של תפיסה סדורה למענה יוכלו לעבור בשלב הזה לתהליך תכנון מפורט למימושם. עבודת המטה לביצוע תהליך זה תתקיים במנהלת המטה. התהליך יכלול את אבני הדרך הבאות:

ניסוח תפיסת המענה – ניסוח מלא של תפיסת המענה תוך שימוש בתבנית מוגדרת שתכלול:

- פרוט מרכיבי המענה היסודיים, כולל: ניסוח עקרונות הפעולה למימוש המענה (עיקרי התו"ל), פירוט עקרוני של מרכיבי הטכנולוגיה העיקריים שיידרשו לצורכי המענה ופירוט ראשוני של משאבי האנוש הדרושים למימוש המענה;
- ניתוח החליפיות של היכולת מול יכולות קיימות (הצעת מקורות חליפיים);
- תרשים לוח זמנים למימוש המענה;
- פירוט תקציבי לתהליך הקמת היכולת;
- פירוט תקציבי של תפעול ותחזוקת היכולת למשך כ-10 שנים.

פירוק המענה למרכיבי יסוד לבניין הכוח – פירוק משנה של היכולת הנדרשת למרכיבי היסוד של בניין הכוח. ניתוח זה יכלול התייחסות למרכיבים הבאים:

יכולות מבצעיות	תשתיות
• תורת הלחימה • כוח אדם - בעלי תפקידים, גיוס • טכנולוגיה ואמצעים • הטמעה, אימונים והכשרות	• לוגיסטיקה • המשאב הכספי • ארגון • מתקנים

גיבוש פרויקטים – בשלב זה מתבצעת אינטגרציה למסגרת פרויקטים שמימושם השלם ירכיב את המענה הנדרש. בכלל זה התייחסות למרכיבים הבאים:

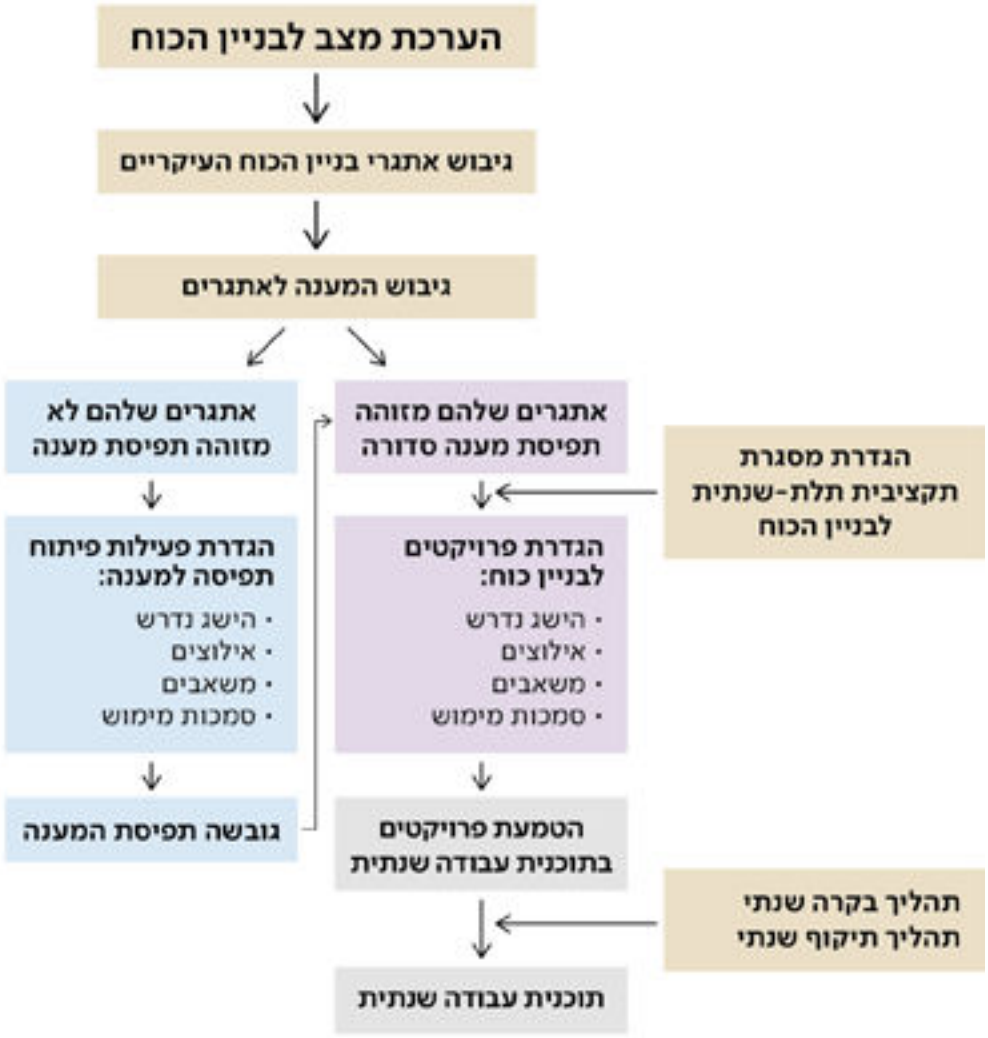
- **ההישג הנדרש** – פירוט של התוצר שאותו נדרש להשיג;
- **האילוצים** – פירוט האילוצים לביצוע הפרויקט;
- **משאבים** – פירוט המשאבים שיועמדו לצורכי מימוש הפרויקט;
- **סמכות הביצוע** – חלק זה יגדיר במפורט את גורם הסמכות למימוש הפרויקט.

5.5 הטמעת הפרויקטים בתוכנית העבודה השנתית ובקרה

שילוב תוכנית העבודה השנתית בהתאם לאבני הדרך שנקבעו לצד ביצוע תהליכי בקרה מתמשכים על בניין הכוח.

5.6 תרשים זרימה לתהליך

התרשים להלן מספק את המתווה העקרוני בתהליך התכנון לבניין הכוח:



5.7 סיכום ביניים

אחת לשלוש שנים מתבצע תהליך הערכת מצב ותכנון לבניין הכוח כפי שפורט לעיל. ייתכנו מקרים שבהם ישתנה התעדוף של אתגר בניין כוח מסוים, יוצף אתגר בניין כוח חדש, או שיבוטל צורך קיים. מקרים אלה ייתכנו הן בשל אירוע המשנה את נקודת העבודה, בשל השתנות הסיכונים או זיהוי הזדמנויות. לצורך זה יתקיים תהליך תיקוף שנתי שיכלול את המרכיבים הבאים: בחינת השינויים בתמונת המצב, בחינת התקפות של האתגרים שהוגדרו בתהליך הערכת המצב, בחינת תקפות הפרויקטים של בניין הכוח שהוגדרו והנמצאים בשלבי מימוש שונים.

6 סיכום

תכנון רב-שנתי לבניין כוח אינו עניין של שיפור הדרגתי, אלא תחרות על עצם היכולת להכריע בסביבה של אי-ודאות מתמדת. הארגונים שיצליחו בעשור הקרוב הם אלה שיבינו כי בניין הכוח חייב להיות דינמי, מודולרי ומבוסס נתונים ולא מושתת על מבנה תכנון נוקשה.

התובנות המרכזיות העולות מהניתוח לעיל הן שמהפכת המידע משנה את כללי המשחק: בינה מלאכותית וסריקת אופק הן כלים חשובים בתהליך. הארגון שיצליח לשלב AI בצורה אחראית ויעילה יזכה ליתרון משמעותי בזיהוי פערים ובקבלת החלטות מהירה. האיום ההיברידי מחייב גישה הוליסטית אמיתית: אין עוד משמעות לתכנן "נגד טרור" או "נגד תקיפות סייבר" בנפרד. העתיד שייך ליכולות גמישות שיכולות להתמודד עם שילובים מורכבים של איומים.

כוח אדם נשאר הגורם המכריע: למרות ההתקדמות הטכנולוגית, האיכות האנושית – גיוס, הכשרה, שימור ופיתוח מנהיגות – היא עדיין ההבדל בין ארגון בינוני למצטיין. הארגונים המובילים כבר משקיעים משאבים עצומים במיומנויות חדשות (מבצעים, סייבר, ניתוח נתונים, חשיבה מערכתית) וביצירת תרבות ארגונית של למידה מתמדת.

תכנון מבוסס יכולות הוא אחד הכלים להתמודדות עם אי-ודאות: במציאות שבה האיום הבא עלול להיות בלתי צפוי, התכנון צריך להתמקד ב"מה אנחנו צריכים להיות מסוגלים לעשות" ולא רק ב"נגד מי או נגד איזה איום אנחנו מתכוננים". גישה זו מעניקה גמישות קריטית.

לסיכום, תכנון רב-שנתי לבניין כוח הופך להיות אחד המרכיבים החשובים ביותר בבניין החוסן. הארגונים שיצליחו לשלב בין חשיבה ארוכת טווח, שימוש חכם בכלים מתקדמים, גמישות מבנית ותרבות ארגונית לומדת – הם אלה שיהיו מוכנים לאתגרי העשור הבא. המסמך מדגיש כי ההצלחה טמונה לא רק במודלים ובתהליכים, אלא ביכולת ליישם אותם בצורה עקבית, אחראית ומתוחכמת בסביבה משתנה במהירות.

© כל הזכויות שמורות
סיוון תשפ"ו / מאי 2026

מכון ירושלים לאסטרטגיה ולביטחון
אבא אבן 16 בשדרת הנשיא השישי, ירושלים
www.jiss.org.il
info@jiss.org.il

אל״מ (מיל׳) פרופ׳ גבי סיבוני היה ראש תכנית צבא ואסטרטגיה ותכנית ביטחון סייבר במכון למחקרי ביטחון לאומי בין השנים 2006-2020. במסגרת זו הוא ייסד שני כתבי עת אקדמיים בתחומים המחקר האמורים. בין עיסוקיו הוא משמש כיועץ לצה״ל ולגופי ביטחון אחרים כמו גם לתעשייה הביטחונית. סיבוני הוא בעל תואר ראשון ושני בהנדסה מאוניברסיטת תל אביב ותואר שלישי במערכות מידע גיאוגרפיות מאוניברסיטת בן גוריון שבנגב.

סיימון ציפיס בעל תואר דוקטור במדעי מדינה ויחסים בינלאומיים מאוניברסיטת בון בגרמניה ותואר שני במדעי המדינה וביטחון לאומי מאוניברסיטת תל אביב. הוא מומחה לטרור, ביטחון סייבר ופוליטיקה פוסט-סובייטית במזרח אירופה ובאירו-אסיה.

www.jiss.org.il