



סייבר ישראל

מערך הסייבר הלאומי



תרגול בסייבר

בנייה ועריכה של תרגילי סייבר לארגון



סייבר ישראל

מערך הסייבר הלאומי



תרגול בסייבר

בנייה ועריכה של תרגילי סייבר לארגון

ספטמבר 2020

מסמך זה נכתב ע"י מערך הסייבר הלאומי לצורך קידום הגנת הסייבר במשק הישראלי. כל הזכויות שמורות למדינת ישראל - מערך הסייבר הלאומי. המסמך נכתב כשירות לציבור. מומלץ ליישם את ההמלצות המפורטות במסמך זה. אין המערך אחראי לכל נזק שייגרם כתוצאה מיישום ההמלצות. הערות והתייחסויות למסמך ניתן להעביר למייל: tora@cyber.gov.il



5	פתח דבר
6	פרק א': יסודות התרגול
6.....	מושגי יסוד
7.....	שיטות תרגול
8.....	מתכונות תרגול
8.....	תרגיל שולחני (TTX - TABLE TOP EXERCISE)
9.....	משחק ארגוני
10.....	תרגיל תפעולי
11	פרק ב': תיק התרגיל
11.....	מבוא
11.....	מתווה התרגיל
12.....	התרחיש
14.....	בניית התרחיש - עקרונות מנחים
15.....	הידיעה התרגילית
17.....	קובץ הידיעות התרגיליות, תגובות המתורגלים לידיעות וה"שעון" התרגילי
19	פרק ג': ניהול התרגיל
19.....	מנהלת התרגיל - יחידת התרגילים של הארגון
21.....	סביבת התרגול
22.....	הבטיחות בתרגיל
23.....	הכנה טכנית ולוגיסטית של סביבת התרגול
23.....	תדרוך המתורגלים לפני התרגיל
25	פרק ד': תחקור התרגיל והפקת לקחים ממנו
25.....	התחקיר - להלכה
26.....	התחקיר - למעשה
28.....	הפקת הלקחים
28.....	תיעוד התהליך
30	נספח א': קווים מנחים לבניית מתווה של תרגיל סייבר
30.....	כללי
30.....	מתווה התרגיל - ותכנית התרגילים הארגונית
30.....	תהליך בניית המתווה
31.....	קביעת מטרת התרגיל
32.....	קביעת מתכונת התרגול
33.....	אישור מתווה התרגיל - ופרסומו
34.....	פרסום חוזר של מתווה התרגיל
35	נספח ב': קווים מנחים לבניית תרחיש של תרגיל סייבר
35.....	כללי
35.....	מנגנון הבנייה של התרחיש
36.....	נקודות תורפה ארגוניות - ותקיפתן
37.....	"רעש" תרגילי
38.....	"תקיפת סייבר" מול "אירוע סייבר" - וגזירת הידיעות התרגיליות מן התרחיש



נספח ג': קווים מנחים לעריכה של תרגיל סייבר שולחני ומשחק ארגוני בסייבר40

- 40כללי
- 40 מסגרת הזמן הכללית
- 40 סביבת התרגול
- 41 ניהול התרגיל
- 42 הכנה טכנית ולוגיסטית של סביבת התרגול

נספח ד': קווים מנחים לעריכה של תרגיל סייבר תפעולי43

- 43 מסגרת הזמן הכללית
- 43 סביבת התרגול
- 44 ניהול התרגיל
- 45 הכנה טכנית ולוגיסטית של סביבת התרגול



קדמה <<<<

מרחב הסייבר הינו מרחב של אפשרויות והזדמנויות בהיבטי קדמה טכנולוגית, קישוריות, שילוביות וחיבור גלובאלי לרשת האינטרנט. מנגד, המרחב מהווה קרקע לאיומים וסיכונים.

מתקפות סייבר עלולות לפגוע בארגונים ולהסב להם נזקים כלכליים ותדמיתיים ניכרים.

על מנת שארגון יהיה מוכן להגן על עצמו מפני איומי סייבר, עליו לשלוט במספר רב של התמחויות - טכנולוגיות, ארגוניות ותהליכיות.

מוכנות ארגונית היא עניין דינאמי, ולפיכך, יש לבחון אותה מעת לעת. אחד הכלים המרכזיים העומד לרשות הארגון לצורך כך הינו **התרגיל**. כבעולמות אחרים, כך גם בעולם הסייבר, עריכת תרגילים מהווה מפתח חשוב לשימור ולקידום של חוסנו של הארגון. מדריך ראשוני וייחודי זה נועד לשמש את ארגוני המשק ככלי עזר בסיסי לבניית תרגילי סייבר, לעריכתם ולהפקת לקחים מהם במתודה סדורה.

בהצלחה לכולנו!

ניצן
ראש אגף בכיר תשתיות עמידות
עמר



פתח דבר <<<<

העקרונות והכללים לתכנונו, לבנייתו ולעריכתו של כל תרגיל באשר הוא אינם תלויים בתחום המקצועי שבו הוא נעשה. מהבחינה הזו, תרגול הוא פעילות גנרית. אולם, בעוד שהעקרונות והכללים הם גנריים, יישומם בתחום מקצועי כלשהו אינו כזה, אלא מושפע מן התחום המדובר. בראייה זו, כפי שיוסבר בהמשך הדברים, יש משמעות לביטוי "תרגיל סייבר", שכן, לתרגול בתחום הזה יש מאפיינים המייחדים אותו מתרגול בכל תחום אחר. מדריך זה מניח בסיס מושגי לעיסוק בתחום התרגול - בכלל, ובתחום הסייבר - בפרט, מציג את העקרונות והכללים לתכנון, בנייה ועריכה של תרגיל סייבר ולתהליך הפקת הלקחים ממנו, ומתייחס בקצרה גם לבנייה של תכנית תרגילים שנתית ורב-שנתית. מושא ההתייחסות שלו הוא הארגון היחיד, וההקשר הרחב יותר של תוכנו הוא המאמץ הכולל של הארגון לקיום, לשימור ולקידום של חוסנו בסייבר.

בהתאם לכך, המדריך בנוי משתי חטיבות: החטיבה הראשונה מכילה את גוף המדריך, ובו הבסיס המושגי כמצויין לעיל. החטיבה השנייה מתמקדת בסוגיות נבחרות מתוך גוף המדריך, ומספקת קווים מנחים לתרגום הדיון המושגי בהן למונחים פראקטיים. היא בנוייה מארבעה נספחים, העוסקים, לפי סדרם, בארבעת הנושאים הבאים:

- בניית מתווה של תרגיל סייבר.
- בניית תרחיש של תרגיל סייבר.
- עריכת תרגיל סייבר שולחני ומשחק ארגוני בסייבר.
- עריכת תרגיל סייבר תפעולי.

חשוב לציין, כי בדומה לתחומים מקצועיים אחרים, המומחיות הנדרשת לבניית תרגילי סייבר ועריכתם ניתנת לרכישה רק בדרך של התנסות מעשית מתמדת. המדריך הזה על שתי חטיבותיו מספק לקורא את הבסיס העיוני הנחוץ לצורך עיסוק מעשי בתחום.

פרק א': יסודות התרגול

מושגי יסוד

תרגיל הוא אחד מסוגי הפעילות שנועדו לקיים, לשמר ולקדם את החוסן הארגוני. כדי להבין כהלכה את תכליתו, יש, קודם לכול, להכיר ולהבין את עולם המושגים שבתוכו הוא מצוי, ומן הראוי לפתוח בשניים: כשירות ומוכנות.

כשירות (Competence) היא היכולת של פרט או של מסגרת ארגונית לממש תפקוד¹ מסויים. **מוכנות (Readiness)** היא היכולת של מסגרת ארגונית לבצע משימה ספציפית וקונקרטית (כך, למשל, על מנת שצוות IR [Incident Response] יוכל לבצע כל אחת ממשימותיו הקבועות המוגדרות לו כמסגרת ארגונית, כל אחד מאנשיו צריך להיות כשיר לבצע את התפקודים הנדרשים ממנו כדי למלא את חלקו בכל אחת מהמשימות הללו).

כשירות מבטאת יכולת גנרית, יסודית (בהמשך לדוגמה הנ"ל, ייתכן שכשירות מסויימת של איש צוות IR משרתת את ביצוען של משימות קבועות אחדות של הצוות, ואולי אף נדרשת למילוי משימות קבועות של מסגרות אחרות בארגון). לעומת זאת, מוכנות מבטאת יכולת המוכוונת כלפי צורך או מטרה מסויימים, ובמקרים רבים היא מותאמת לזירת התרחשות או לסביבת פעולה מסויימת. כמו כן, היא לעולם תכונה של מסגרות וארגונים שלמים, ולא של פרטים.

מוכנות נשענת כל-כולה על כשירויות - אלא שאין מדובר בכשירויות של אנשים או של צוותים בלבד, אלא גם של אמצעים ומשאבים (כלומר, תקינות של אמצעים וזמינות של משאבים ברמות המלאי הנדרשות).

הכשירות והמוכנות של הפרט והארגון הן תכונות המחייבות בנייה הדרגתית, שימור שוטף וקידום בהתאם לצורך ועל פי תכנון. האחריות הכוללת לביצוע כל אלה מוטלת על הנהלת הארגון. שני הכלים המרכזיים המשמשים את הארגון לצורך כך הם **הכשרה (Training) וריענון (Refresher)**². הכשרה מעניקה ובונה יכולות, וריענון משמר אותן. לפיכך, התוצר העיקרי של שני אלה הוא שיפור היכולת של הפרט או המסגרת הארגונית לתפקד ולמלא את משימותיהם. הכשרה וריענון ממומשים, הלכה למעשה, באמצעות קורסים, השתלמויות וימי עיון.

ככל פעילות אחרת, גם פעילות ההכשרה והריענון של הארגון מחייבת בקרה. הודות לכך שכשירות ומוכנות הן מושגים בני-מדידה - כמותנית (Quantitative), ככל שהדבר אפשרי, ובכל מקרה אחר - איכותנית (Qualitative), ניתן להעריך את רמתן באמצעות מדדים שהוגדרו ונקבעו מראש. הארגון נעזר, אפוא, במדדים אלה כדי לוודא שמופעי ההכשרה והריענון הם **אפקטיביים** (כלומר, שהם אכן משיגים את מטרותיהם), ושהם עושים זאת **ביעילות** (כלומר, תוך מיצוי מיטבי של המשאבים שהושקעו לצורך כך). מבחינה תפעולית, בקרה זו מבוצעת באמצעות שני סוגי פעילות: **ביקורת ותרגיל**.

¹ המונח "תפקוד" מובא כאן במובן של "פונקציה".

² ישנה מידה של אי-בהירות בהמשגה ובמינוח - הן בעברית והן באנגלית - בתחום ההדרכה. על כל פנים, בתחום הצבאי והביטחוני נהוג להשתמש בביטוי "אימון" לציון כל פעילות של הכשרה או שמירת כשירות. בראייה זו, אפוא, אימון הוא הכלי המרכזי לבניית כשירות ומוכנות.

ביקורת היא פעילות ניהולית, שהתוצר העיקרי שלה הוא תמונת מצב עדכנית של הגוף המבוקר בתחומים שבהם הוחלט שהוא ייבדק. מעצם טבעה, ביקורת היא פעילות שיפוטית: הגוף המבוקר מוערך בשורה של ציונים, הנקבעים על פי המדדים שצוינו לעיל. מובן, לפיכך, שביקורת היא כלי חיוני בבקרה של פעילויות ההכשרה והריענון של הארגון. לעומת זאת, **תרגיל** הוא פעילות לימודית, שנועדה להפקה של תובנות ולקחים שאימוצם ויישומם ישפרו את כשירותו ומוכנותו של הארגון. מכך נובע, שתרגיל אינו כלי שיפוטי, ועריכתו מכוונת כל-כולה לסייע לארגון, ולא להעמידו בסיטואציה מאיימת כלשהי. יתירה מזאת, הגם שהן ביקורת והן תרגיל נועדו ללמידה ארגונית, הרי שגורם מבוקר נוטה לתפוס את תוצרי הלמידה המופקים ממנה כהתערבות מטרידה בענייניו הפנימיים, או אף כשוט או כלי ניגוח בידי הסמכות העורכת את הביקורת; לעומת זאת, גורם מתורגל לומד באמצעות התנסות אישית, המעודדת אותו להזדהות עם תוצרי הלמידה ולאמצם.³ מאפיינים אלה של התרגיל, ובוודאי השוני המהותי בינו לבין ביקורת, הינם חשובים ביותר, ועליהם לא רק לעמוד אל מול עיניהם של מתכנני התרגיל ועורכיו ממועד יזום התרגיל ועד למועד סיום הפקת הלקחים ממנו, אלא גם להיות מוכּנים היטב למתורגלים לאורך כל הדרך הזו.

להלן תובא שורה של הבחנות בין הדרכים שבהן ניתן לתרגל, ולאחריה יידון לפרטיו אופן השימוש בהן. מן הראוי להקדים ולומר, שכל תרגיל באשר הוא מתבסס על הדמיה (סימולציה) של מצבים ונסיבות שעשויים להתחולל במציאות.⁴ "לערוך תרגיל" פירושו, הלכה למעשה, לחשוף את המתורגלים באופן מבוקר לפרטיה של הסימולציה הזו, ולנהל את תגובתם להם על פי עקרונות וכללים דידקטיים.

שיטות תרגול

ישנן שתי שיטות לביצוע תרגול: **עיונית - ומעשית**:

בשיטה העיונית המתורגלים נדרשים להתמודד חשיבתית עם אתגרים שאין להם מענה מן המוכן עבורם, לעיתים קרובות תוך הפגנת תושייה ויצירתיות ו"חשיבה מחוץ לקופסה". פעילותם של המתורגלים מבוססת על שיח (דיונים והתייעצויות בצוותים). הם אינם מגיבים בפועל להתרחשויות המוצגות להם, אלא מצהירים (לרוב - על פה, ולעיתים בכתב) אודות מה שהיו עושים אילו היה מדובר בהתרחשות אמיתית. ככלל, תרגול בשיטה הזו נערך כשכל המתורגלים מכונסים באתר אחד, תוך שהם מאורגנים בקבוצה אחת או יותר.

בשיטה המעשית המתורגלים נדרשים להתמודד עם האתגרים המוצגים להם באמצעות פעילות הקרובה ככל הניתן לזו שבה היו נוקטים אילו היה מדובר בהתרחשויות אמיתיות. הם אינם מצהירים מילולית - אלא **פועלים**. ככלל, תרגול בשיטה הזו מתבצע כשכל מתורגל פועל בסביבת התפקוד האמיתית שלו. גם בשיטה הזו המתורגלים מקיימים



³ במסגרת עריכה של ביקורת מקובל לערוך פעילות שנהוג לכנותה "תרגיל פתע". על יסוד האמור לעיל יובן, כי אין מדובר בתרגיל כלל, אלא במעין "מבחן מעשי" המבוסס על סימולציה.

⁴ מעצם טבעם, תרגילים נוטים להישען במידה רבה על סימולציה. אחת הסיבות המרכזיות לכך היא ההכרח להימנע מגרימת נזקים כתוצאה משימוש במרכיבי אמת מתוך סביבת התפקוד של המתורגל. **בממד הסייבר, עניין זה הוא רגיש במיוחד.** דיון מפורט בסוגיית הסימולציה בתרגיל יובא בהמשך המדריך.

ביניהם לבין עצמם שיח, אך זה אינו מוגבל להתייעצויות ודיונים, אלא ממומש על בסיס דרכי התקשורת שנועדו לכך במצב האמת. הטבלה שלהלן מרכזת את היתרונות והחסרונות של שתי השיטות:

היתרונות והחסרונות של שתי שיטות התרגול		
השיטה	תרגול עיוני	תרגול מעשי
יתרונות	"זול" למימוש - צורך מזערי באמצעי עזר. מאפשר מיקוד במרכיבים "רכים" של הארגון (תפיסה, מדיניות, מתודולוגיה). מצריך הכנה קצרה, יחסית. פשוט לניהול. בעל סיכון נמוך לתפקוד הארגון ולמערכותיו.	מאפשר תרגול יעיל ואפקטיבי של התפקוד הארגוני בכל הרמות, בהיקף רחב, וביעילות רבה.
חסרונות	אינו מאפשר תרגול של התפקוד הארגוני מעבר לרמת הפרט (התרגול הוא "סטאטי" באופיו).	"יקר" למימוש - עתיר משאבים. מצריך הכנה ארוכה ומורכבת, יחסית. מורכב לניהול. בעל סיכון גבוה למערכות הארגון.

- בהמשך לכתוב בטבלה הנ"ל, מומלץ להשתמש בתרגול עיוני כאשר:
- מדובר בתרגיל ראשון (אי-פעם, או בתחום הנוגע בדבר) עבור הארגון כולו או עבור בעלי תפקיד מרכזיים בו.
 - הארגון בוחן את הצורך לבצע שינוי מבני (בין אם כזה הנובע מעדכון הייעוד או משימות קבועות של הארגון, ובין אם לאו).
 - הארגון בוחן את הצורך לבצע שינוי תהליכי, או כל סוגיה עקרונית אחרת הנוגעת לתפקוד הארגון.
- לעומת זאת, מומלץ להשתמש בתרגול מעשי כאשר:
- מדובר בארגון "צעיר", יחסית, אך כזה שהנהלתו מעריכה כי הגיע כבר לבשלות תפעולית, ומבקשת לבחון הערכה זו.
 - הארגון יישם באחרונה שינוי תהליכי או מבני, ומבקש לבחון את נכונות השינוי או את הצלחת תהליך יישומו.
 - הארגון מזהה פערים מהותיים באפקטיביות או ביעילות של תפקודו, ומבקש לנצל את פוטנציאל האבחון של התרגיל כדי לנתח את הבעיה וללמוד כיצד לפתור אותה.

מתכונת תרגול

כל אחת משיטות התרגול המנויות לעיל ניתנת למימוש במתכונות מסויימות. המתכונת (Setting) מבטאת את האופן שבו תיושם שיטת התרגול הנבחרת. הגם שהמתכונת אמורה להתבסס על אחת מהשיטות המתוארות לעיל, ניתן - ואף מקובל - לשלב בה מרכיבים מהשיטה האחרת. להלן יובאו, תחילה, שתי המתכונות העיקריות לביצוע **תרגול עיוני**.

תרגיל שולחני (TTX - Table Top Exercise)

במתכונת זו, המתורגלים מכונסים בצוות אחד או יותר, וכל אחד מהם מסב אל שולחן אחד ומנהל רב-שיח אודות אופן ההתמודדות עם אתגרים/בעיות המוצגים לו, בדרך כלל



במסגרת של סיפור מעשה "מתגלגל". מבנה הצוותים עשוי לשקף מבנה ארגוני אמיתי; לחליפין, הם עשויים להיבנות כ-"Think Tanks", כדי לאפשר סיעור מוחות ולעודד חשיבה יצירתית בסביבת תרגול המשוחררת מאילוץ היום-יום.

המתורגלים מגיבים לתרחיש שהם נחשפים אליו באופן הצהרתי (בדרך כלל, ההצהרות האלה נאמרות בחלל החדר, אולם ניתן גם לתעד אותן בזמן-אמת כחלק מהשיח השוטף של המתורגלים). יצוין, שהתרחיש במתכונת הזו הוא מודמה לחלוטין ("מתודי", כמו שמקובל לכנות זאת).

בהיות התרגיל מכשיר שנועד לאפשר למידה, לנתוניה של תמונת המצב התרגילית בנקודת הסיום שלו יש חשיבות משנית - החשיבות העיקרית נודעת לתפקודם של המתורגלים, ולא לתוצאותיו.

השימוש העיקרי בתרגיל השולחני בסייבר הוא לצורך הגברת המודעות הכללית מפני איומי סייבר, שינון והפנמה של מושגים, ותיקוף של תכניות פעולה ונהלים. בתוך כך, ניתן להסתייע בו כדי לזהות חוזקות וחולשות מהותיות במערך ההגנה של הארגון מפני תקיפות סייבר. ככזה, הוא מתאים במיוחד לתרגול דרגי הארגון הפועלים ברמה האופרטיבית והאסטרטגית שלו.

בשל מאפייניו והנסיבות שבהן הוא נערך, השליטה בביצוע של תרגיל שולחני פשוטה, ולפיכך, הוא נחשב לכלי עבודה "מדויק", במובן שקל, יחסית, לעמוד במטרות שהוצבו לו מלכתחילה.

משחק ארגוני⁵

בדומה לתרגיל שולחני, גם במשחק הארגוני פועלים מספר צוותים של מתורגלים, המתמודדים עם תרחיש (מודמה) הולך ומתפתח. בשונה מתרגיל שולחני, המשחק הארגוני הוא למעשה "משחק תפקידים" (ומכאן גם שמו), שכל המשתתפים בו מהווים, יחדיו, מערכת: אופייני הוא, שכל צוות שכזה מייצג גוף או ארגון מסויים (או אפילו מדינה שלמה). יחסי הגומלין בין הצוותים וחבריהם מוגדרים מראש (ועשויים להיות ידידותיים, תחרותיים או עוינים), ותפקודם מונע ומבוקר באמצעות כללים שאף הם נקבעו מראש (הגם שחלקם עשוי להיות נסתר מידיעת המתורגלים לאורך חלק מהמשחק או עד סופו).⁶ בשל אופיו וטבעו של המשחק הארגוני, ולהבדיל מהמקרה של תרגיל שולחני, לתוצאות תפקודם של המתורגלים בו יש, לעיתים קרובות, משמעות כשלעצמן, ולפיכך, הן עשויות להוות מרכיב חשוב בהפקת הלקחים ממנו.

מנקודת הראות של הארגון היחיד, הוא נועד בעיקר לתרגול גורמים פנימיים בדרג האופרטיבי והאסטרטגי בארגונים גדולים, יחסית.

המתכונת העיקרית המשמשת לביצוע תרגול מעשי היא התרגיל התפעולי, כמפורט להלן.

⁵ בעולם הרחב מקובל לכנות את המשחק הארגוני בשם – "משחק מלחמה" (War Game).

⁶ בשל טיבו של מערך יחסי הגומלין במשחק הארגוני, אופייני הוא שבין המתורגלים בו ישורר מתח מובנה, אשר מגרה את המתורגלים לחשוב ולפעול (מתודית, כמובן), ויוצר אוירת תחרות המסייעת ללמידה.



תרגיל תפעולי

במתכונת זו, המתורגלים פועלים בסביבת התפקוד האמיתית שלהם, על מרכיביה ותנאיה. הודות למאפייניה ולנסיבות שבהן היא נערכת, מתכונת זו מאפשרת תרגול החל מהרמה הטכנו-טקטית, שבה המיקוד הוא בתחומי התמחות אישיים וצוותיים (בעיקר באמצעות תרגילי "Hands-On")⁷, וכלה ברמה האסטרטגית, שבה מדובר בתרגול מערכתי ורחב-היקף ברמה הפנים-ארגונית והרב-ארגונית, והמיקוד הוא בתהליכי קבלת החלטות, בתהליכי עבודה, בממשקים בין גופים ויחידות, בנהלים ובסוגיות של מדיניות. בתרגול תפעולי ניתן, אומנם, לעשות שימוש במרכיבי תרחיש אמיתיים⁸, אולם לרוב מדובר בשימוש מוגבל מאוד ובהיקף קטן, יחסית.

מבלי להפחית כהוא-זה מחשיבותו ומנחיצותו של תרגול ברמה הטכנו-טקטית, אין ספק שהמיצוי המרבי של הפוטנציאל הטמון במתכונת התפעולית הינו ברמה האופרטיבית והאסטרטגית. לפיכך, יתמקד הדיון מכאן ואילך ברמות אלה, ופירוט נוסף באשר לרמה הטכנו-טקטית יובא בנספח ד' למדריך.

תנאי מרכזי להבטחת האפקטיביות של תרגיל תפעולי הוא, שמצרך הגורמים המתורגלים ייצג נאמנה את הארגון בכללותו. קיומו של התנאי הזה נובע מהעובדה, שלעולם לא ניתן לתרגל את הארגון כולו, ומשמעותו היא, שהלקחים שיופקו מהתרגיל אכן יהיו רלוואנטיים לארגון בכללותו, למרות שרק חלק ממנו תורגל בפועל, כאמור.⁹

⁷ תרגילי "Hands-On" מיועדים לבעלי תפקיד העוסקים בהיבטים הטכניים והטכנולוגיים של ההגנה בסייבר – אנליזה, Incident Response, Reversed Engineering, וכיו"ב. האפקטיביות שלהם מצריכה, בדרך כלל, שימוש באמצעי סימולציה ייעודיים.

⁸ הכוונה כאן היא לנקיטת פעולות אמיתיות ביחס למרכיבים אותנטיים של הארגון, ובעיקר – לתקיפת אמת שלהם בסייבר, או, לחליפין – לפגיעה אמיתית כלשהי בהם באמצעים אחרים.

⁹ חשוב לחדד, שמילוי התנאי הזה אין משמעותו, בהכרח, לשאוף לכך שמירב הארגון יתורגל. במילים אחרות, מדובר כאן בשאלה של מהות ואיכות, ולא של כמות.



פרק ב': תיק התרגיל

מבוא

תרגיל הוא סוג של מבצע, ולכן, כדי שמימושו ישיג את מטרותיו, נדרש לתכננו מראש. תכנית זו היא **תיק התרגיל**, וזה כולל את המרכיבים הבאים:

- מתווה התרגיל.
- התרחיש.
- קובץ הידיעות התרגיליות.
- להלן יפורטו שלבי ההכנה של מרכיבים אלה על פי סדרם.

מתווה התרגיל

מתווה התרגיל, כפי ששמו מעיד עליו, הוא אוסף של כל המאפיינים הקובעים את מהותו ודמותו של התרגיל, והם מובאים להלן על פי סדר קביעתם:

- מטרת התרגיל.
- הרכב המתורגלים.
- מטרות המשנה של התרגיל.
- נושאי התרגול.
- מתכונת התרגול.
- המחווון התרגילי.

מעצם היותו כזה, המתווה צריך להיקבע במסגרת הבנייה של תכנית התרגילים השנתית/רב-שנתית של הארגון. שאר מרכיביו של תיק התרגיל יוגדרו לקראת מועד עריכתו של התרגיל עצמו (עוד על כך - בנספח א' למדריך).

מטרת התרגיל מבטאת את כוונתו של הארגון לבחון מרכיבים או היבטים מסויימים של מוכנותו בנקודת זמן נתונה. לפיכך, נכון יהיה שהגורמים האחראים לקיומם ולשימור רמתם הנאותה של אלה יוגדרו כ**מתורגלים**.

הגורמים המתורגלים אמורים לממש אחריות זו באמצעות שורה של משימות קבועות וייעודיות, שלכל אחת מהן מוגדר הישג נדרש. יוצא מכך שכל הישג שכזה מהווה גם **מטרת משנה** של התרגיל¹⁰. **נושאי התרגול** ייגזרו ממטרות המשנה.¹¹

יסוד חשוב בקביעתה של מטרת התרגיל הוא **כלל ההיפוך בין האמצעים למטרה בתרגיל**. במצב האמת, הארגון מממש ככל יכולתו את מוכנותו כדי להשיג את מטרותיו העסקיות ולהגשים את ייעודו. בתרגיל, לעומת זאת, רמת המוכנות הארגונית היא זו שנמצאת במוקד העניין, והתרגיל נועד, למעשה, לבחון באיזו מידה יש בכוחה לאפשר לארגון להשיג את מטרותיו וייעודו. במילים אחרות, המטרה התרגילית מתמקדת בבחינת האמצעים הארגוניים ("איך"), בעוד שהמטרות והייעוד של הארגון ("מה") באים לידי

¹⁰ יודגש, שלתרגיל יש להגדיר מטרה אחת ויחידה, ובסימן האמרה "תפסת מרובה – לא תפסת", מומלץ לגזור מתוכה שלוש מטרות משנה לכל היותר.

¹¹ בהמשך לנאמר בעניין מטרות המשנה, מומלץ להגדיר שלושה נושאי תרגול לכל היותר.

ביטוי בתרגיל בעקיפין, באמצעות אותן משימות קבועות שנזכרו לעיל, שלכל אחת מהן נקבע על ידי הארגון הישג נדרש.

כאמור, תרגיל אינו פעילות שיפוטית ביסודה. יחד עם זאת, מובן מאליו שהישגיהם של המתורגלים הם מידע חיוני להשגת מטרת התרגיל, שכן, רק על פיהם ניתן יהיה להעריך את מצב מוכנותו של הארגון. מדידת הישגיהם של המתורגלים והערכתם צריכות להיעשות על פי **מדדי הכשירות והמוכנות** שהוגדרו בארגון בתחומי התפקוד הנוגעים בדבר. לפיכך, יש לכלול בתיק התרגיל אוסף של כל המדדים הרלוואנטיים למטרות התרגיל ונושאי התרגול הנגזרים מהן. אוסף זה מכונה בשם **מחון תרגילי**.

בהתייחס לאופן השימוש במדדים האלה, יש לזכור שלרוב לא מדובר במדע מדויק, ולכן, פעולות המדידה וההערכה מחייבות נקיטת זהירות רבה. ישנם כלים שונים שביכולתם לסייע במזעור מידת העיוות (Bias) של תמונת הכשירות והמוכנות שתתקבל בסוף התהליך (כגון - מהימנות בין שופטים), אך אין זה המקום להרחיב את הדיון בתחום המקצועי רחב-היריעה הזה.

בהמשך לאמור לעיל, חשוב להדגיש כי בנייתו של מתווה עבור תרגיל מסויים אינה עומדת לעצמה - כל תרגיל אמור להיות חוליה בשרשרת מתמשכת של מופעים כאלה, שתכליתה היא, כפי שכבר הוסבר, לקיים, לשמר ולקדם את המוכנות הארגונית להתמודדות עם אירועי ומשברי סייבר. הדבר משפיע ישירות על הקביעה של רמת הדרישות שיציב כל תרגיל כשלעצמו בפני המתורגלים (המצב האופטימלי הוא, בראייה כללית ועקרונית, שכל תרגיל מציב דרישות גבוהות יותר מקודמו). מרכיב מרכזי בעיצוב המתווה של תרגיל נתון הוא לקחי כל התרגילים שכבר בוצעו לפניו (עוד על עניין זה - בהמשך).

בעוד שהמתווה מבטא את מה שהארגון מעוניין ללמוד מן התרגיל, המרכיב של תיק התרגיל שמאפשר בפועל את הלמידה הזו הוא ה**תרחיש**.

התרחיש

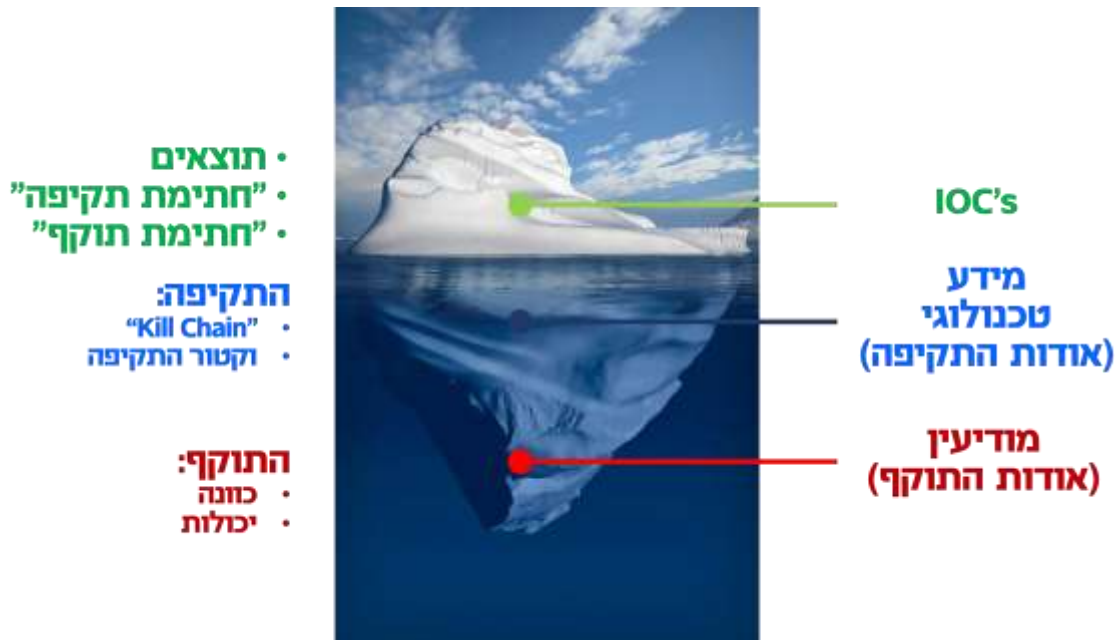
התרחיש הוא ה"עלילה" של התרגיל, והדברים שקורים במסגרת שלה הם הגירויים שעליהם המתורגלים אמורים להגיב במהלכו.¹² התרחיש צריך להיות מציאותי, מתקבל על הדעת ומאתגר (עוד על כך - בנספח ב'). אבן הבניין היסודית של התרחיש היא **תקיפת סייבר**. תרחיש עשוי להכיל תקיפה אחת או יותר, אך מומלץ שמספר התקיפות הכולל לא יעלה על חמש. **בהגדרה, לכל תרגיל יש תרחיש אחד ויחיד**. יחד עם זאת, התרחיש עשוי להיבנות כסדרה של מספר "עלילות", שכל אחת עומדת לעצמה ללא כל קשר לאחרות. במקרה שכזה, כל עלילה תכיל תקיפת סייבר אחת לפחות.¹³

תרשים מס' 1 שלהלן מביא את "מודל הקרחון" - מודל של תקיפת סייבר - משתי זוויות ראייה: זו של התוקף, וזו של המגן. מזווית הראייה של התוקף, מדובר במהלך שנועד להשיג מטרה שהוא הגדיר, המשרתת את כוונותיו, וזאת, תוך שהוא מנצל את יכולותיו בתחום. התקיפה מייצרת תוצאים (אפקטים) גלויים שונים, המתחוללים בתוך מערכותיו

¹² כוחם של הדברים האמורים להלן יפה לכל מתכונות התרגול.

¹³ תרחיש מהסוג הזה מתאים בעיקר לתרגול עיוני (תרגיל שולחני או משחק ארגוני). בתרגול מעשי קיימת חשיבות רבה להדמיה אפקטיבית של מציאות אפשרית, ולפיכך, התרחיש המתאים ביותר לצורך כך הוא עלילה רצופה אחת.

של המגן, ומתבטאים בשיבושים בתפקודן, ולרוב - גם בסימנים גלויים אחרים, המעידים על קיומה ("חתימות"¹⁴ שונות של גורמי אנוש ואמצעים המעורבים בתקיפה).



תרשים מס' 1: מודל ה"קרחון"

מזווית הראייה של המגן, הוא נחשף לשורה של סממנים (IOC's¹⁵), המעידים על האפשרות להתרחשותה של תקיפת סייבר. אלה כוללים את כל התוצאים והסימנים הנזכרים לעיל (שהרי הם גלויים למגן), אולם, צפוי שבעיני המגן רבים מהם יהיו נטולי הקשר, שכן, הם מעידים על פעילות שמעצם טבעה נעשית בחשאי. סממנים אלה מיוצגים בתרשים בדמות קצה הקרחון ("תשיעית העליונה שלו") הצף על פני המים, ובהיותו כזה - הוא גם גלוי לעין-כל. לעומת זאת, כל המידע האחר אודות התוקף והתקיפה, השרוי בעמקי מרחב הסייבר הנתקף, מגולם בדמות שמונה התשיעיות האחרות של הקרחון, השקועות בעומק הים ונסתרות מעין-רואים.

בראייה תרגילית, אפוא, המידע הזה הוא בגדר סוד תרגילי, ופרטיו ייודעו למתורגלים (קרי: המגינים) רק בשני מקרים: האחד - כשהמתורגלים הסיקו אותם בכוחות עצמם על סמך הידיעות שקיבלו; והאחר - הם נחשפו למתורגלים ביוזמה של מנהלי התרגיל (הרחבה בעניין המקרה הזה תובא בהמשך). הדינמיקה התרגילית מתמצית במאמציו של המתורגל להתגבר בהצלחה על האתגרים שהתרחיש מעמיד בפניו, תוך התמודדות מתמדת עם מחסור במידע, עם מידע לא רלוואנטי ועם ידיעות סותרות (לפחות לכאורה). הדינמיקה הזו מתקיימת בשני מישורים בעת ובעונה אחת: המישור התפעולי (תהליכים ארגוניים - מבצעיים, עסקיים או אחרים) והמישור הטכנולוגי (תהליכים המתרחשים בתוך מרחב הסייבר). כמובן, קיימת זיקה חזקה בין שני אלה, שכן, ייעודן של תשתיות התקשוב של

¹⁴ בביטוי "חתימה" הכוונה היא למידע הקשור בדרך זו או אחרת לפעולותיו של התוקף, אשר נחשף לידיעת המגן (כמו, למשל: "ירוט" של התייחסות שנעשתה במסגרת שיח ב-Darknet לארגון או לנכס סייבר שלו שיש לו ייחוד; או Port Scan הנעשה בתדירות גבוהה אל מול נכס סייבר מסויים שלו).

¹⁵ Indicators Of Compromise.

הארגון הוא לתמוך בתהליכים התפעוליים השונים שלו, וכשאלה מותקפות, סופם של התהליכים התפעוליים להיפגע.¹⁶

המצב הדואלי הזה מהווה בסיס להיווצרות של דילמות תפקודיות (לא רק בתרגיל, אלא גם בחיים האמיתיים): כך, למשל, עשוי הממונה על הגנת הסייבר בארגון להמליץ להנהלה להשבית באופן יזום תהליך תפעולי מסויים, כדי להקטין את "משטח התקיפה" הארגוני לנוכח התפתחויות אפשריות של התקיפה המתחוללת כבר; ההנהלה, מצידה, עשויה להתנגד למהלך שכזה, מתוך אינטרס עסקי מובהק.¹⁷

כדי להבטיח שהתרגיל ישיג את מטרתו, האתגרים שהתרחיש יעמיד מול המתורגלים צריכים לעלות מתוך נושאי התרגול, ולעורר את המתורגלים לפעול בתחומים הקשורים ישירות למטרות המשנה של התרגיל (עוד על כך - בנספח ב').

לאמיתו של דבר, תרשים מס' 1 מתאר תמונה חלקית של מבנה התרחיש. שכן, במציאות של ממד הסייבר, מה שנראה כקצה קרחון המזדקר מעל פני המים עשוי להתברר (במבט בוחן מקרוב, כלומר, לאחר בירור נאות) כתלולית של קצף הנישאת בראש גל גדול. ובלשון פחות ציורית: לא כל מה שמסתמן כתקיפת סייבר הוא אכן כזה. לאור זאת, ולצורך בנייה של סימולציה הקרובה ככל הניתן למציאות, יש לשבץ בתרחיש גם אירועים "תמימים" (כגון - קלקולי מערכת או תקלות תפעוליות). בעגה של תחום התרגילים מכנים מרכיב זה בשם "רעש".

בניית התרחיש - עקרונות מנחים

- **משקלו של מרכיב הסייבר בתרגיל:** התרחיש צריך להעמיד מול המתורגלים אתגר בתחום הגנת הסייבר לאורך התרגיל כולו, וזאת, מבלי למעט בחשיבותו של ההיבט התפעולי של התרגול.¹⁸
- **מציאותיות:** התרחיש צריך לשקף למתורגלים את המציאות המוכרת להם, וזאת - עד הפרטים הקטנים ביותר. הדברים אמורים לא רק במידע אודות מה שקורה בסימולציה התרגילית, אלא גם בהתפתחויות החלות בה כתוצאה ישירה מתפקודם של המתורגלים המהווה תגובה לה. דבר זה נחוץ כדי להבטיח שהמתורגלים יתנו אמון במה שמסופר להם, והודות לכך, יחושו הזדהות עם הסיטואציה המתפתחת בתרגיל ויתפקדו בתוכה "באופן טבעי", דהיינו - באופן הקרוב ביותר לאופן שבו היו פועלים, לו היו הדברים המסופרים מתרחשים במציאות. מסיבה זו, מומלץ לשתף בתהליך בניית התרחיש נציגים של היחידות הארגוניות המתורגלות, שהינם בעלי מומחיות בנושאי התרגול.¹⁹
- **חומרה:** כשמה כן היא - מידת החומרה של המצב הכללי של הארגון, כפועל יוצא של הנזקים המצטברים והולכים הנגרמים מתקיפות הסייבר הכלולות בתרחיש. מלכתחילה, בניית התרחיש צריכה להתחשב בתוצרי תהליך הערכת הסיכונים

¹⁶ כוחם של דברים אלה יפה לעולם ה-IT ולעולם ה-OT כאחד.

¹⁷ בהקשר זה ראוי להזכיר את חשיבותו של ניהול הסיכונים בעת משבר סייבר, ובתוך כך, את הערכת ההשפעה של מהלך תקיפת סייבר על התהליכים העסקיים של הארגון (BIA – Business Impact Assessment).

¹⁸ דיון מורחב בעניין זה מובא בנספח ב'.

¹⁹ מומחה שכזה יהיה מנוע מלהשתתף בתרגיל, כיוון שנחשף מראש לפרטי התרחיש. עדיף להתמודד עם הדילמה "מתורגל או שותף-סוד תרגילי?" לפני התרגיל, מאשר לעמוד בפני עובדה מוגמרת בעת עריכתו.



וניתוחם שביצע הארגון.²⁰ בראייה זו, "מרכז הכובד" של התרחיש יתבסס על אותה תקיפות שייכללו בו, שתוחלת הנזק שלהן מוערכת כגבוהה. בתוך אלה, חשוב שתהיה לפחות אחת, שההסתברות להתרחשותה מוערכת כנמוכה.

- **קושי:** הניסיון האנושי מלמד, שכישלונות מניעים ללמידה במידה גדולה יותר מהצלחות.²¹ לפיכך, יש לבנות את התרחיש כך שיקשה על המתורגלים במידה כזו, שסיכוייהם להיכשל לפחות בחלק מהמאמצים שלהם יהיו קרובים לוודאיים. מחד גיסא, רמת הקושי של התרחיש צריכה להיות גבוהה דיה כדי להוציא את המתורגלים מ"אזור הנוחות" שלהם, ובדרך זו, להניע אותם להשקיע מאמצים בהתמודדות עם האתגרים שהוא מעמיד בפניהם; מאידך גיסא, עליה להיות נמוכה דיה כדי למנוע תסכול של המתורגלים אל מול אתגרי התרחיש - דבר שסופו ליטול מהם את המוטיבציה להשקיע מאמצים שכאלה.²²

- **סיפור רקע:** הדיון בתרחיש עד כה התבסס על ההנחה שהוא ייחשף למתורגלים רק בזמן עריכתו של התרגיל. מבלי לסתור זאת, ניתן להקדים לכך פרסום של סיפור רקע. מדובר במקבץ של ידיעות, שחלקן מכיל מידע הנוגע לתקיפות הסייבר שיתחוללו בתרגיל, וחלקן הוא בגדר "רעש". בכל מקרה, סיפור הרקע לא יכיל מידע שנכלל כבר בתרחיש. הרעיון מאחורי המרכיב הזה, הנתון לבחירה, הוא לעודד את המתורגלים להתחיל בהיערכות לתרגיל עצמו, וליצור בקרבם מתח וציפייה לקראתו. לפיכך, אם אכן משתמשים בסיפור רקע, מומלץ להפיץ אותו למתורגלים כשבוע לפני מועד התרגיל. בהגדרה, סיפור הרקע מהווה חלק בלתי נפרד ממתווה התרגיל, הגם, כאמור, שהוא מופץ במועד נפרד ממנו.

- **עיוותים תרגיליים:** גם בהתמלא כל הציוויים המנויים לעיל, נותרת בעינה מגבלה אחת שהטוב בתרחישים לא יוכל להימנע מקיומה ומהשפעתה: התרחיש מאפשר לערוך סימולציה של המציאות - אולם, אין בנמצא סימולציה שבכוחה להוות תחליף מושלם למציאות. יוצא מכך, שלמעשה בכל תרגיל יחולו עיוותים מסויימים ביחס למה שצפוי שיתרחש בנסיבות זהות בחיים האמיתיים. הנזק המשמעותי ביותר הטמון בעיוותים אלה מאיים בעיקר על תקפותם של הלקחים שיופקו מן התרגיל (ועל כך - הרחבה ופירוט בהמשך). אי-לכך, מתחדד הצורך בבנייה של תרחיש שלא זו בלבד שיבטא באופן הנאמן ביותר את האתגרים שעומדים למתורגלים אמורים להתמודד, אלא גם יוכל "להתגלגל" באופן שישקף את המציאות שבה הם רגילים לתפקד בחיי היום-יום שלהם.

הידיעה התרגילית

בהסתמך על המתואר קודם לכן, התרחיש של התרגיל אינו אלא אוסף ה"קרחונים" שנבנו

²⁰ ישנן גישות שונות להערכת הסיכונים שמשקפים לארגון (ללא קשר לתחום הסייבר באופן ספציפי). מדובר, כמובן, בנושא חשוב ביותר, אך העיסוק בו חורג מגבולות הדיון של מדריך זה, ולכן לא יורחב כאן הדיבור בעניינו.

²¹ בהקשר זה יהיה אך הולם לצטט את אמרתו המפורסמת של ווינסטון צ'רצ'יל אודות חשיבותו של הכישלון: "Success is all about going from failure to failure without losing enthusiasm."

²² יש לזכור, שישנה זיקה בין מידת החומרה של התרחיש למידת הקושי שלו.

על ידי מתכנני התרגיל, כאשר המציאות המדומה שבתוכה יצטרכו המתורגלים לתפקד מבוססת על אוסף הסממנים המהווים את החלק העליון, הגלוי על פני השטח, של כל "קרחון". אולם, בכך לא די, שכן, כאמור לעיל, בחיים האמיתיים סביר כי הגורמים המתורגלים ייחשפו לפריטי מידע נוספים אודות התקיפות והתוקפים המחוללים אותן. לפיכך, התרחיש עובר תהליך של פריטה (break-down), שבמהלכו מעובדים הן חלקו הגלוי והן פרטים מחלקיו הסמויים לכדי אוסף של **ידיעות תרגיליות. קובץ הידיעות התרגיליות** המתקבל כתוצאה מכך מבטא הן את תקיפות הסייבר והן את אירועי ה"רעש" הכלולים בתרחיש. כאמור, בעוד שתהליך הבנייה של התרחיש נעשה מנקודת ראותו של התוקף, תהליך הפריטה של הידיעות התרגיליות נעשה כולו מנקודת ראותם של המגינים, קרי - המתורגלים.

ידיעה תרגילית היא רשומת מידע בעלת מבנה קבוע, הבא בשתי תצורות: מצומצמת - ומורחבת. בתצורתה המצומצמת, כוללת ידיעה תרגילית את השדות הבאים:

- הגורם המוסר את הידיעה: אחד הגורמים המתורגלים, או גורם שאינו מתורגל.²³
- הגורם הנמען לידיעה (מתורגל, בהגדרה).
- התאריך והמועד ה**תרגיליים** של מסירת הידיעה למתורגלים.
- זמן ה**אמת** של מסירת הידיעה למתורגלים.²⁴
- תוכן הידיעה.

ידיעה תרגילית צריכה:

- לבטא באופן נאמן את התוצא (אפקט) שאמור להיווצר בנקודת הזמן הנדונה בתהליך ההתגלגלות של תקיפת הסייבר/אירוע ה"רעש" התרגילי.
- לא לכלול כל מידע שהוא בגדר סוד תרגילי.
- לבטא באופן נאמן את תהליכי זרימת המידע האמורים או הצפויים להתקיים במקרה של התרחשות אמיתית.

ניתן לתאר את הדינמיקה הכללית של תרגיל כמסע של המתורגלים אל התובנות והלקחים שיופקו בסופו. הגם שתוכנם של אלה האחרונים אינו ידוע, בעיקרו, מראש, מנהלי התרגיל יודעים היטב לאן, באופן כללי, המתורגלים צריכים להגיע בסוף המסע הזה - מטרת התרגיל, מטרות המשנה שלו ונושאי התרגול אמורים לבטא זאת באופן ברור. בראייה זו, הידיעות הנמסרות למתורגלים הן האמצעי בידי מנהלי התרגיל להניע את המתורגלים לבצע את המסע הזה, ולהכווין אותם בדרכם כך שאכן יגיעו אל היעד המבוקש.²⁵ יחד עם זאת, אין ביכולתם של מנהלי התרגיל לשלוט בתגובת המתורגלים לידיעות, ולפיכך, ייתכן מצב שבו המתורגלים יתעו בדרכם או פשוט "ייתקעו" בה ללא יכולת להתקדם. במקרה שכזה, עומד לרשות מנהלי התרגיל טיפוס מיוחד של ידיעה -

²³ יודגש, שבשום מקרה הגורם הזה אינו מנהל התרגיל או מישהו מעוזריו - מדובר אך ורק בגורמים הלקוחים מסביבת האמת התפקודית של המתורגלים. כאמור, חלקם עשויים להשתתף בעצמם בתרגיל; השאר ייוצגו על ידי גורמים שיופעלו על ידי מנהל התרגיל, אשר, בהיותם כאלה, הם שייכים בעצמם לצוות ההנהלה של התרגיל.

²⁴ שדה זה וקודמו יידונו במסגרת הדיון בהרכבת קובץ הידיעות התרגיליות, המובא להלן.

²⁵ ככלל, לא אמור להתקיים שיח ישיר בין מנהלי התרגיל לבין המתורגלים במהלך התרגיל. עוד על כך - בדיון אודות ניהול התרגיל, בהמשך המדריך.

ידיעה מנחה.²⁶ לידיעה מנחה אין מועד מסירה מתוכנן מראש - היא מוחזקת במצב הכן, למקרה הצורך, וכאשר הצורך עולה, או-אז היא נמסרת למתורגלים. ידיעה מנחה היא חלק אורגני מהתרחיש ומעלילת התרגיל, ובעצם מסירתה טמונה הציפייה של מנהלי התרגיל, שהמידע הנמסר באמצעותה יסייע למתורגלים להתקדם כנדרש. אולם, לעיתים גם אמצעי זה אינו מספיק. במקרה שכזה, תידרש התערבות ישירה של מנהלי התרגיל בתפקודם של המתורגלים לצורך קידום העניינים.

קובץ הידיעות התרגיליות, תגובות המתורגלים לידיעות וה"שעון" התרגילי

קובץ הידיעות התרגיליות הוא, למעשה, טבלה, שכל שורה בה מוקדשת לידיעה תרגילית אחת. כפי שניתן כבר להבין מהכתוב לעיל, הקובץ הזה לא אמור להיות אוסף אקראי של פיסות מידע - אלא שרשרת מובנית של מסרים, שמבטאת באופן נאמן את התפתחות האירועים הכלולים בתרחיש (הן תקיפות והן "רעשים"), ושמעבר לכך, גם לוקחת בחשבון את התגובות הצפויות של המתורגלים אליהם. דבר זה יסייע למנהלי התרגיל לשלוט בהתפתחותו ובמהלכיו.

לשם כך, יש למפות מראש את התגובות של המתורגלים לכל ידיעה. יש להבחין בין תגובה **רצויה** - לצפויה. התגובה הרצויה מבטאת את הדרך הראויה והנכונה להתמודדות עם נתוני המצב שמציגה הידיעה (ברוח הביטוי המוכר "פתרון בית ספר"). **המחונן התרגילי** עשוי לסייע רבות בקביעתה. התגובה הצפויה, לעומת זאת, משקפת את מה שככל הנראה יעשו המתורגלים בפועל - והיא מבוססת על ההיכרות של מנהלי התרגיל עם המתורגלים ועם המצב הקיים בכללותו. חשוב לציין, שאין הכרח למלא את שני השדות הללו בתוכן עבור כל ידיעה. לעיתים, יהיה נכון ומתאים לבטא שינוי משמעותי בתמונת המצב התרגילית באמצעות רצף של מספר ידיעות, שרק בסופו (כלומר, בידיעה האחרונה שלו) יהיה טעם להגדיר את תגובות המתורגלים לנתונים החדשים שנמסרו להם.

על יסוד כל זאת, הידיעות ערוכות בקובץ הידיעות התרגיליות **בתצורה המורחבת** שלהן, המכילה שני שדות נוספים על אלה המרכיבים את התצורה המצומצמת:

- התגובה **הרצויה** של המתורגלים לידיעה.
- התגובה **הצפויה** של המתורגלים לידיעה.²⁷

הצורך לשלוט במהלכי התרגיל ובהתפתחותו מחייב גם להתייחס בהרכבת הקובץ הזה לעניין ה"שעון התרגילי".

התרחיש התרגילי עשוי לשרטט מציאות מודמית (simulated) המתרחשת בתאריך ובשעות שונים מאלה המתקיימים בפועל (זמן אמת). התאריך והשעות שנקבעו בתרחיש מכוונים, אפוא, בשם "שעון תרגילי", והוא מקבל את ביטויו בפועל בתזמון הידיעות. לרוב (ובוודאי כשמדובר בתקיפות סייבר), פרק הזמן האמיתי המוקדש לתרגיל הוא קצר

²⁶ בלשון הדיבור המקובלת בתחום, נהוג לכנות ידיעה מנחה בשם "ידיעת מגירה" או "ידיעה נצורה".
²⁷ למען הסר ספק, קובץ הידיעות התרגיליות משמש את מנהלי התרגיל לשליטה במהלכיו, ותוכנו אינו נחשף, כפי שהוא, למתורגלים. הידיעות הכלולות בו מועברות אליהם בפועל בתצורה המצומצמת שלהן (כלומר, ללא השדות "תגובה רצויה" ו"תגובה צפויה", כאמור לעיל). טכנית, ניתן להעבירן באמצעים שונים, הן ידנית והן באופן ממוכן.



משמעותית מזה שלאורכו האירועים שבתרחיש מתחוללים במציאות. כדי להתגבר על הקושי הזה, נדרש "לכווץ" את משכי הזמן האמיתיים שהיו נדרשים להגיב במציאות על הקורה בתרחיש, ולהקצות למתורגלים פרקי זמן קצרים יותר משמעותית לצורך תגובה על הידיעות שהם מקבלים. כך, הידיעות מתוזמנות, למעשה, פעמיים: פעם אחת, באמצעות השדה "התאריך והמועד התרגיליים של מסירת הידיעה למתורגלים", ופעם שנייה, באמצעות השדה "זמן האמת של מסירת הידיעה למתורגלים" (כך, למשל, ניתן להעביר למתורגלים שתי ידיעות עוקבות בהפרש זמנים אמיתי של חצי שעה זו-מזו, כאשר ההתרחשויות המתוארות בהן קרו, תרגילית, בהפרש של שתיים עשרה שעות זו-מזו). הפער המתמיד בין שתי סקאלות הזמן הנדונות פה (שצפוי אף לגדול ככל שהתרגיל נמשך) עשוי ליצור בקרב המתורגלים את התחושה שהשעון התרגילי מתקדם ב"קפיצות". לפיכך, מנהלי התרגיל צריכים להשתדל שה"קפיצות" האלה תהיינה כמה שפחות חדות.

באשר למידת ה"כיווץ", צריך לקחת בחשבון את פרק הזמן (האמיתי) שנכון יהיה להקצות למתורגלים כדי להגיב לכל ידיעה. הקצאת פרק זמן קצר מדי עלולה לפגום באפקטיביות של התרגול, ולכן, יש להימנע מכך ככל שניתן. בהקשר זה, מן הראוי לדון בנטייה מקובלת של מנהלי תרגיל להעמיס משימות על המתורגלים, כדי לבחון את תפקודם בתנאי עקה (stress). על כך יש לומר, תחילה, שעקה אינה בהכרח תולדה של **כמות** המידע שאתו צריכים המתורגלים להתמודד, אלא של **משמעות** המידע הזה, ולכן, יש להתמקד בעיצוב נכון של תוכן הידיעות ולא במספרן לשם השגת תכלית זו. אך מעבר לכך, תפקוד בתנאי עקה הוא מיומנות בסיסית ובעיקר אישית, ולפיכך, התרגול שלה רלוואנטי בעיקר לשיטה המעשית, קרי - לתרגילים תפעוליים, וליתר דיוק (משיקולים מתודולוגיים ודידאקטיים) - לכאלה הנערכים ברמה הטכנו-טקטית של הארגון. אלא שבמקרה הזה המרחק בין תרגול המיומנות הזו לבנייתה הוא קטן למדי, ולפיכך, מומלץ לארגון לטפל בה באמצעות פעולות הכשרה (כמו, למשל, במסגרת של הכשרת מנהלים).

כלל גדול בעולם התרגילים הוא לעולם לא להעתיק באופן מוכני תיק תרגיל קיים לצורך עריכת תרגיל חדש. תרגול הוא אחת מהדרכים האפקטיביות ביותר לאלץ את הארגון לצאת מ"אזור הנוחות" שלו - והודות לכך, להקטין את הסכנה להיווצרות קיבעון תפיסתי ולהפיכה של אורחי התנהגות מקובלים לדפוסי פעולה "מקודשים".



פרק ג': ניהול התרגיל

מנהלת התרגיל - יחידת התרגילים של הארגון

עד כה, נעשה במדריך שימוש בביטוי "מנהלי התרגיל". אכן, תרגיל אינו נבנה או מתנהל בעצמו. לשם כך קיימת **מנהלת תרגיל** (ובקיצור: "המנהלת"). מנהלת של תרגיל הנערך בממד הסייבר עומדת על ארבע רגליים:

- מתודולוג (שלרוב משמש גם כראש המנהלת).²⁸
- טכנולוג (הטכנולוג אחראי, בהגדרה, גם למודיעין אודות **התקיפות**).²⁹
- מומחה תהליכים.
- (במקרים מסוימים) מומחה למודיעין אודות **התוקפים**.³⁰

לרוב, תכלול מנהלת התרגיל בעלי תפקיד נוספים, ועל כן, ארבעת בעלי התפקיד הנ"ל יכוננו, להלן, בשם **הצוות המוביל** של התרגיל.³¹

במונח "מנהלת התרגיל" הכוונה היא, אם כן, למסגרת ארגונית ייעודית וזמנית, אשר מוקמת לקראת מועד עריכתו של תרגיל מסויים שנקבע בתכנית העבודה, ומפורקת עם סיום תהליך הפקת הלקחים ממנו. למעשה, לצורך הבנייה של תכנית התרגילים השנתית של הארגון (הכוללת בתוכה בין השאר, כפי שכבר הוסבר, את המתווה של כל אחד מן התרגילים שנקבעו בה), די בצוות מצומצם, הכולל אדם אחד או שניים לכל היותר. מכאן, שראוי ונכון כי הצוות המצומצם יהווה יחידה קבועה של הארגון, שתישא באחריות לניהול כלל פעילות התרגול שלו באופן שוטף. להלן, יתייחס הכתוב ליחידה הזו בשם "יחידת התרגילים" (של הארגון), כדי להבדיל אותה מהגוף המכונה "מנהלת (ה)תרגיל". בראייה זו, יחידת התרגילים תהווה את הגרעין שסביבו תוקם המנהלת של כל תרגיל ספציפי. ככלל, המנהלת מדמה כל בעל תפקיד וכל גוף או ארגון שאינם משתתפים בפועל בתרגיל. על מנת להיערך מראש לתגובה על התפתחויות צפויות - ובעיקר מזדמנות - של מהלכי התרגיל, ניתן להלכה לייצג את אלה באמצעות ידיעות שהוכנו מראש. הלכה זו אכן ניתנת להפיכה למעשה במקרים רבים של תרגול עיוני. אולם, בתרגול מעשי עשויות ההתפתחויות האפשריות במהלכי התרגיל להצריך הכנה מראש של מספר גדול של ידיעות שכאלה. יתר על כן, הצורך בהעברה מתוזמנת כהלכה שלהן למתורגלים רבים בתוך פרקי זמן קצרים עלול ליצור עומס בלתי נסבל על המנהלת. לפיכך, מומלץ וגם נהוג

²⁸ לרוב צפוי שראש יחידת התרגילים הארגונית ישמש כראש המנהלת. יחד עם זאת, ובעיקר משיקולים ייצוגיים, ימונה לתפקיד הזה עובד בכיר יותר מתוך הארגון.

²⁹ הכוונה כאן היא בעיקר למה שמכונה במקומותינו בשם "מודיעין כחול", דהיינו - למידע שעיקרו טכנולוגי, ושחלק ניכר מהעיסוק בו מצוי, בהקשר לממד הסייבר, הן בידי הארגונים הנתונים לתקיפות סייבר, והן בידיהם של גורמי אבטחת סייבר מסחריים (מקומיים ובין-לאומיים) המתמחים בכך.

³⁰ כהשלמה לכתוב בהערה הקודמת, הכוונה כאן היא בעיקר למה שמכונה "מודיעין אדום", דהיינו - כזה המצוי תחת האחריות של קהילת המודיעין הלאומית. הגם שבימינו הגבולות בין שני עולמות המודיעין האלה מטושטשים לעיתים קרובות, לגרמי הקהילה עדיין יש, כמובן, יכולות ייחודיות משמעותיות.

³¹ כפי שיפורט בהמשך הפרק, מאפייניו הייחודיים של מרחב הסייבר מציבים מלכתחילה מגבלות ניכרות על היכולת לכלול בתרחיש פעולות התערבות אמיתיות - הן ביוזמת המנהלת, והן ביוזמת המתורגלים. יחד עם זאת, על המנהלת לשקול מינוי של **בקר בטיחות**, שיפקח על הפעילות המתרחשת בפועל במהלך התרגיל, וימנע היווצרות של נסיבות שעלולות לסכן את מרחב הסייבר הארגוני בכל צורה שהיא.

להפעיל לצורך כך במהלך התרגיל בעלי תפקיד ייעודיים, המכונים **תפקידנים**.³² התפקידנים הם בעלי תפקיד אמיתיים, הן מתוך הארגון המתורגל והן מחוצה לו. בתרגיל, מוטל עליהם לייצג את עצמם, או את הגוף/ארגון שהם משתייכים אליו. במובן הזה, ניתן לחלקם לשתי קבוצות משנה: כאלה שיש למתורגלים סמכות כלשהי כלפיהם, או שהם מהווים עמיתים פנים-ארגוניים או חוץ-ארגוניים שלהם; וכאלה שיש להם סמכות כלפי המתורגלים (כך, למשל, בתרגיל המיועד להנהלת חברה, הקבוצה הראשונה עשויה לכלול עובדים שונים של הארגון, ועובדים של ארגונים המהווים ספקים של הארגון המתורגל; והקבוצה השנייה - את הדירקטוריון של החברה, דרגי הנהלה בכירים שאינם מתורגלים, או רגולטור מדינתי כלשהו). בהתחשב בכך שישנם קווי דמיון מסויימים בין פעילותו של תפקידן לבין זו של מתורגל, הדעת נותנת שגם תפקידן עשוי לצאת נשכר מן התרגיל, למרות שלא היה בין המתורגלים. במקרה שכזה, מדובר ב"בונוס" משמח. כך או כך, התפקידנים הם חברי מנהלת לכל דבר ועניין.

במעקב שלה אחר התפקוד של המתורגלים, מסתייעת המנהלת **בתצפיתנים**.³³ התצפיתן נוכח פיסית בסביבת התרגול, ועורך תצפית בלתי משתתפת במהלכיהם של המתורגלים הפועלים בה. הוא ממלא שני תפקידים: במהלך התרגיל - קישור שוטף בין המנהלת לסביבת התרגול בעת התרגיל, ולאחר סיומו - דיווח מסכם אודות תפקוד המתורגלים לאורך כל משך משימת התצפית שלו. כמו התפקידנים, גם התצפיתנים הם חברים מן המניין במנהלת התרגיל.

תשתיות סימולציה
ואמצעי המחשה



תצפיתנים



תפקידנים



כמצויין לעיל, הצוות המוביל והתצפיתנים לא אמורים, ככלל, להתערב בתפקוד המתורגלים. למעשה, על המנהלת להשתדל להיות "שקופה" ובלתי מורגשת ככל האפשר מבחינתם. לכלל זה שני חריגים:

- כפי שכבר הוסבר, משלא עלה בידי המנהלת להכווין בנקודת זמן מסויימת את פעילות המתורגלים על פי התכנית שלה גם לאחר שימוש בידיעות מנחות, יש מקום להתערבות ישירה שלה בתפקוד המתורגלים לצורך הזה. בהקשר זה ראוי לציין, שהמנהלת חותרת להשגת מטרת התרגיל, ולא לכך שכל הידיעות שהכינה עבור המתורגלים אכן יימסרו להם עד תום התרגיל.
- המתורגלים רשאים לפנות למנהלת בשאלות הנוגעות לכללי הניהול של התרגיל (למשל, בנוגע לשעון התרגילי, לתכולת התפקיד שמגלם תפקידן מסויים, וכיו"ב).³⁴

³² בלשון הדיבור המקובלת בתחום התרגילים, נהוג לכנות בעלי תפקיד אלה בשמות "בקרה נמוכה" ו"בקרה גבוהה", בהתאמה.

³³ בלשון הדיבור המקובלת בתחום התרגילים נהוג לכנותם (למרבה הבלבול והצער) בשם "בקרים".

³⁴ להבדיל, ובהתאם למה שכבר הוסבר, צפוי ומצופה שהמתורגלים ימצאו באינטראקציה שוטפת עם התפקידנים.

סביבת התרגול

סביבת התרגול היא זו שבה המתורגלים פועלים. קיים הבדל מהותי בין סביבת התרגול שמשמשת לתרגול עיוני, לבין זו המשמשת לתרגול מעשי: בתרגול מעשי השאיפה היא, כאמור, שהמתורגלים יפעלו בתוך סביבת התפקוד האמיתית והטבעית שלהם. מכאן גם נובע, שסביבת התרגול תשתרע בדרך כלל על פני אתרים אחדים, שלפחות חלק מהם יכילו יותר מחלל תפקוד אחד. לעומת זאת, בתרגול העיוני השאיפה היא ליצור תנאים שיעודדו חשיבה משוחררת מאילוצי היום-יום, ולפיכך, אופייני הוא שהמתורגלים יפעלו במסגרת הזו בסביבה "מלאכותית", שעיצובה מונחה על ידי שיקולים דידיאקטיים וגם לוגיסטיים, כך שברוב המקרים אין לה קשר וזיקה לסביבת התפקוד האמיתית שלהם. היא תכיל, בדרך כלל, חלל אחד - האולם או החדר שבו התרגיל ייערך. במקרה שמתכונת התרגול הספציפית כוללת עבודה בצוותים, תכלול סביבת התרגול חללי עבודה נוספים. שיקול נוסף שיש בו כדי להשפיע על עיצוב סביבת התרגול העיונית הוא ביטחון מידע, דהיינו - רמת הסיווג הביטחוני של החומר התרגילי. כך, ייתכן שיהיה צורך ביצירת אזורי תרגול ממודרים, שיאפשרו חציצה בין צוותי עבודה שונים.



הבדל נוסף בין שתי שיטות התרגול בהיבט זה הוא משקלם ומשמעותם של אמצעי הסימולציה. בהיבט הלימודי, בתרגול מעשי אך טבעי הוא לרצות לבצע תקיפת סייבר בפועל על מערכות התקשוב של הארגון. למרבה הצער, שאיפה זו מוגבלת על ידי שיקולים חוקיים ומשפטיים, בטיחותיים, חומריים, כלכליים ותדמיתיים. הפתרון המתבקש, לכאורה, לבעיה זו הוא שימוש בתשתית תקשוב או בסביבת רשת נפרדים ויעודיים לצרכי תרגול, שידמו באופן נאמן את המבנה והתפקוד של תשתיות התקשוב האמיתיות של הארגון. בראש ובראשונה, פתרון שכזה הוא בדרך כלל יקר (ומחייב אחזקה ועדכון מתמידים, כדי שימשיך לייצג נאמנה כל שינוי או עדכון במרחב הסייבר הארגוני האמיתי). אך מעבר לכך, האפקטיביות שלו תהיה מלכתחילה - ובהגדרה - מוגבלת, שכן, אין באמת אפשרות מעשית לדמות גם את כל התהליכים העסקיים שנשענים על התשתית הזו. במקרים רבים, הדבר יצריך הקמה של "ארגון דמה" שלם. לפיכך, ובוודאי

בהעדר תשתיות סימולציה שכאלה (שזה, מן הסתם, המקרה הרווח), תרגול בסביבת האמת מחייב, לעיתים קרובות, לא רק שימוש מוגבל במרכיביה ובמשאביה, אלא אף שימוש במרכיבים ובאמצעים שיופרדו ממנה וישמשו לצורך התרגול בלבד (מדובר בעקרון פעולה המכונה: "הפרדת סביבת התרגול מסביבת האמת"). לפיכך, בתרגיל תפעולי על המנהלת להקפיד במיוחד לעצב את הידיעות התרגיליות כך שייסעו בהמחשת התקיפה ותוצאיה, ובאופן זה, להבטיח ככל הניתן שהתמונה התרגילית שתצטייר על בסיסן תפצה, ולו באופן חלקי, על העיוותים שפשרה שכזו תיצור בסביבת התרגול.

מעצם טבעו, התרגול העיוני מציב דרישות צנועות יותר בתחום הזה. למעשה, במקרה הזה מדובר יותר על "החייאה" מאשר על "סימולציה" - כלומר, הענקת צביון אותנטי ככל הניתן להתרחשויות המתוארות בידיעות התרגיליות. כך, למשל, ניתן "להחיות" במידה ניכרת ידיעה חדשותית על ידי הקרנת מבזק חדשות, שהופק במיוחד לשם כך, באולם שבו נערך התרגיל.

חשוב לסייג ולומר, שהשימוש בעזרי סימולציה והמחשה נועד מלכתחילה להגביר את הרושם האותנטי שהסיטואציה התרגילית עושה על המתורגלים, וזאת, על מנת לעודד את המתורגלים לתפקד באופן "טבעי", ולא, להבדיל, כדי לשוות לתרגיל חזות מרשימה. בהתחשב בכך שעזרים שכאלה הם משאב יקר, יחסית, מומלץ להימנע ככל האפשר משימוש בהם ליצירת "פירוטכניקה" לשמה, ולהגביל את ההשקעה בהם למקרים ספציפיים בתרחיש המצדיקים זאת.



הבטיחות בתרגיל

מבלי לסתור את האמור לעיל, ובהמשך לנאמר בתחילת הפרק, על מנהלת התרגיל לבחון היטב את התרחיש ואת קובץ הידיעות התרגיליות **בהיבט הבטיחותי**. אם תגיע המנהלת לכלל הבנה, שגלגול התרחיש עשוי לחולל נסיבות שבהן עלול להיווצר סיכון כלשהו למרחב הסייבר הארגוני (דבר העלול, כמובן, לגרום נזק לנכסי סייבר ארגוניים, ואולי אף ליצור נזק אגבי כתוצאה מכך), אזי עליה למנות **בקר בטיחות** לתרגיל.³⁵ בקר הבטיחות יכין **נספח בטיחות** למתווה התרגיל, שיכלול שורה של הוראות המכוונות אל כלל המשתתפים בתרגיל, שתכליתן למנוע את היווצרות הסיכונים האמורים לעיל, ולהנחות את המשתתפים כיצד לפעול, במקרה שסיכון כלשהו התממש בכל זאת.

³⁵ בכל מקרה שבו יוכר קיומם של סיכונים שכאלה, על המנהלת לבצע תהליך של ניתוח סיכונים, ולקבוע את תצורתם הסופית של התרחיש וקובץ הידיעות התרגיליות בהתאם לתוצאותיו. כמו-כן, תהליך אישורו של מתווה התרגיל יכלול את אישור ההיערכות הבטיחותית לקראתו, תוך מתן תשומת לב נאותה לדגשים המתאימים.

הכנה טכנית ולוגיסטית של סביבת התרגול

תרגול עיוני נבדל מתרגול מעשי בהיבט הטכני והלוגיסטי. עניין זה יידון לגופו במסגרת הנספחים המצורפים למדריך. יחד עם זאת, יש לשתי המתכונות האלה גם מאפיינים משותפים בהקשר הזה, כמפורט להלן:

- מומלץ להקליט (בווידאו, ואם לא ניתן, אז לפחות באמצעי שמע) את מהלך התרגיל. יהא התייעוד של התצפיתנים טוב ככל שיהיה, הם לעולם לא יוכלו לתעד בכתב את כל הנאמר. לאחר התרגיל, יש לסקור את כל החומר המוקלט, ולמצות ממנו את כל המידע הדרוש לשם תחקור התרגיל. רצוי לעשות זאת בתוך שבוע ימים ממועד עריכתו של התרגיל.
- רצוי להימנע מהכנסת דברי מאכל ואמצעים להכנת משקאות חמים למרחב התרגיל, ולהסתפק במים ומשקאות קלים. זאת, על מנת למנוע ככל האפשר את הסחת הקשב של המתורגלים. יחד עם זאת, רצוי להציב מחוצה לו, ובמקום נגיש וקרוב, עמדה שתכלול כיבוד קל. בתרגיל שמשכו מגיע לחצי יום, מומלץ להעמיד בסיומו לרשות המשתתפים ארוחת צהריים קלה. בתרגילים שמשכם מגיע לימים אחדים, יש לוודא שמילוי צרכי ההסעדה של המשתתפים לא יפריע למהלך התרגיל, ובהתאם לכך, לספק להם באופן יזום ומתוכנן מראש מזון ומשקה ככל הנדרש.
- הגישה למקום עריכת התרגיל היא חשובה ביותר. לפיכך, יש לשלוח למשתתפים הוראות הגעה ברכב פרטי ובתחבורה ציבורית כשבוע לפני מועד האירוע. לכך יש לצרף מידע אודות סידורי החנייה הזמינים במקום.
- לעיתים מזומנות תצריך עריכת התרגיל שירותי אבטחה ייעודיים - הן בתחום הפיסי והן בתחום בטחון המידע. על המנהלת לכלול בתיק התרגיל תכנית אבטחה סדורה, ולוודא את מימושה כנדרש בעת עריכת התרגיל.³⁶

תדרוך המתורגלים לפני התרגיל

תרגיל הוא, אחרי ככלות הכל, סוג של משחק, וככזה, הוא נערך ב"מגרש" מוגדר, ועל פי כללים קבועים מראש. לפיכך, יש חשיבות רבה לכך שהמתורגלים יכירו היטב את המגרש התרגילי ואת כללי הפעולה בו לפני מועד עריכת התרגיל. לצורך כך, על המנהלת לערוך תדריך למתורגלים. מן הראוי לשוב ולהזכיר כאן, כי יש לציין בתדריך את העובדה שהתרגיל אינו כלי שיפוטי מכל סוג שהוא.³⁷ עיתוי התדריך ודגשיו תלויים בשיטת התרגול:

- בתרגול עיוני, ניתן להסתפק בתדריך קצר (עד 15 דקות) שיינתן בפתח התרגיל. במהלכו, מומלץ לערוך הצגה פומבית של המשתתפים (הכוונה היא בעיקר לאלה היושבים אל שולחן התרגול - למקרה שיש משתתפים נוספים, הממוקמים אחרת).

³⁶ בצד ההיבט הביטחוני של התרגול, יש לו גם היבט בטיחותי. מאחר ותקיפות הסייבר בתרגיל אמורות להיות מוזמנות, ולאור העובדה שנדרשת מלכתחילה הקפדה על הפרדת סביבת התרגול מסביבת האמת, ההיבט הבטיחותי בא לידי ביטוי בעיקר במקרה שבתרגיל כלולות פעילויות פיזיות, הכרוכות בסיכונים בטיחותיים.

³⁷ בהקשר זה, מקובל להגדיר באנגלית את סביבת התרגול כ-"No Fault Environment".



חשוב לפרט את לוח הזמנים המלא של התרגיל, ובמקרה שהוא נערך בשני מרחבים פיסיים או יותר - יש לציין זאת במסגרת ההסבר אודות כללי המשחק.

• בתרגול מעשי, שבו לרוב קיים פיזור פיסיוגרפי של המתורגלים, השימוש בוועוד חזותי (Video Conference) מאפשר להתגבר על אילוצי הזמן והמרחב ולערוך את התדריך בפתח התרגיל. במקרה שאמצעי זה אינו זמין, ניתן לערוך שיחת ועידה טלפונית, אולם רצוי להקדים לה תדרוך פנים-אל-פנים שייערך כשבוע לפני מועד עריכת התרגיל. אם ניתן לזמן את כל המתורגלים למקום אחד - אפשר להסתפק בתדריך אחד, אחרת יש לערוך מספר תדריכים שכאלה. בתדרוך לקראת תרגיל מעשי מומלץ להדגיש את עניין דרכי התקשורת התרגיליות, וכן, את כללי הפרדה בין סביבת התרגול לסביבת התפקוד האמיתית של המתורגלים (עוד על עניין זה - בנספח ד').

פרק ד': תחקור התרגיל והפקת לקחים ממנו

התחקיר - להלכה



השכחה האנושית מאיימת על ההשרדות של כל פיסת ידע שלא תועדה, והאפקטים של פעולתה הם מידיים. לכך נלווית נטייה אנושית אחרת, והיא - לשחזר באופן יצירתי את העבר. לפיכך, תהליך הפקת הלקחים מן התרגיל צריך להתחיל מייד עם סיומו. השלב הראשון בתהליך הזה הוא **התחקיר**. כמובן, תחקיר הוא כלי עזר חיוני ללמידה עבור כל פעילות, ולפיכך, ייפתח פרק זה באמירות כלליות הנוגעות לו.

תחקיר (באנגלית - After Action Review, ובקיצור: AAR) הוא בירור של פרטי ביצועה של פעילות מסויימת לאור מטרתה, תוצאותיה והתהליכים שהתחוללו במהלכה, וכל זאת, לשם מיצוי מירב הידיעות והנתונים הדרושים ליצירת בסיס להסקת מסקנות ולהפקת לקחים. ישנם שני טיפוסים תחקיר: **תחקיר פנימי** ותחקיר **מומחים**. תחקיר פנימי (באנגלית: Debriefing) נערך מטעמו של הגוף שהיה אחראי לפעילות המתוחקרת, ומשתתפים בו רק אותם בעלי תפקיד שלקחו בה חלק בכל דרך שהיא. מטרתו - להפיק את מירב התובנות שעלו מן הפעילות, ולעשות זאת בסביבה סגורה ו"ידידותית", שתאפשר שיח פתוח וגלוי. לאור הכתוב בראשית הדברים, חשוב מאוד לערוך את התחקיר הפנימי סמוך ככל הניתן למועד הסיום של הפעילות המתוחקרת, כדי "ללכוד" את הדברים החשובים ביותר הנוגעים לה סמוך ככל הניתן למועד התרחשותם. כך, נהוג לקיים מייד עם סיום הפעילות המתוחקרת **תחקיר ראשוני** (באנגלית, נהוג לכנותו בשם: Hot Wash). לתחקיר הפנימי שני יתרונות עיקריים: ראשית, המידע הנדון בו מבוסס על החוויות של מי שהיה הכי קרוב לפעילות המתוחקרת, ושנית, הלקחים שיופקו על בסיס המידע הזה ישרתו ישירות את מי שצריך להתכונן לפעילות הבאה. כיוון שכך, התחקיר הפנימי הוא כלי למידה ארגונית (וגם אישית) שאין לו תחליף. יחד עם זאת, יש לכלי הזה שתי מגבלות: ראשית, גם באווירת השיח הידידותית ביותר עשויים הדברים הנידונים ללקות בחסר, או לזכות בפרשנות שיש בה עיוות כלשהו. שנית, המשתתפים בתחקיר אינם, בהכרח, המומחים המקצועיים הטובים ביותר בתחומי התוכן המתוחקרים.

לאור זאת, נהוג במקרים רבים להוסיף על התחקיר הפנימי **תחקיר מומחים**. סוג זה של תחקיר נערך בסוגיות שנבחרו על ידי הגוף שביצע את הפעילות המתוחקרת, והוא מבוצע על ידי מומחים מקצועיים לדבר. בד-בבד, יש להקפיד שאיש מבין המומחים האלה לא השתתף בפעילות המתוחקרת.

יודגש, כי יש הכרח לבצע תחקיר פנימי; לעומת זאת, ההחלטה לבצע תחקיר מומחים נתונה לשיקול דעתו של הגוף המתוחקר. במקרה שהפעילות המתוחקרת נוגעת לארגון גדול או למספר ארגונים, מומלץ לבצע תחקיר פנימי במתכונת מדורגת: כל ארגון או גוף שהשתתפו בפעילות מתחקר את עצמו, ומדווח את תוצרי התחקיר שלו לרמה הממונה



עליו. כשמדובר בהיקף ארגוני מצומצם, או בהיעדר זמן מספיק, ניתן עדיין לבצע תחקיר במתכונת אחודה, שבה כלל הגורמים הנוגעים בדבר עורכים את התחקיר הפנימי בצוותא. יצויין, שהתחקיר הראשוני שנזכר לעיל אינו מחליף תחקיר פנימי סדור - בין אם זה ייעשה במתכונת מדורגת או אחודה.

כאמור, כוחם של הדברים הנ"ל יפה לכל פעילות באשר היא. כשמדובר בתרגיל, יש לציין שני מאפיינים מייחדים. ראשית - בהתייחס לתחקיר הראשוני, ומבלי לסתור את הכתוב לעיל, יש לומר כי חברי המנהלת רשאים להשתתף בו, אולם תרומתם הפעילה לשיח צריכה להיות מוגבלת למקרה שהמתורגלים יבקשו לדעת פרטים אודות התרחיש התרגילי ואופן גלגולו בפועל במהלך התרגיל (מדובר בעיקר במידע שהוגדר מלכתחילה כ"סוד תרגילי", כך שמן הסתם לפחות חלק ממנו נותר סמוי מן המתורגלים גם בסוף התרגיל). למען הסר ספק, אין זה בסמכותה או מתפקידה של המנהלת לבקר את תפקודם של המתורגלים, ולמעט החריג שצויין קודם לכן, עליה להימנע מלהתערב בדרך כלשהי בתהליכי התחקור של התרגיל.

שנית - מנהלת התרגיל, כמוה כמתורגלים, נדרשת לקיים תחקיר סדור משלה, ועניינו - בחינת המידה שבה התרגיל אכן הצליח למלא את המטרות שנקבעו לו. גם התחקיר הזה יתנהל בפורום פנימי (וללא השתתפות של המתורגלים).

התחקיר - למעשה

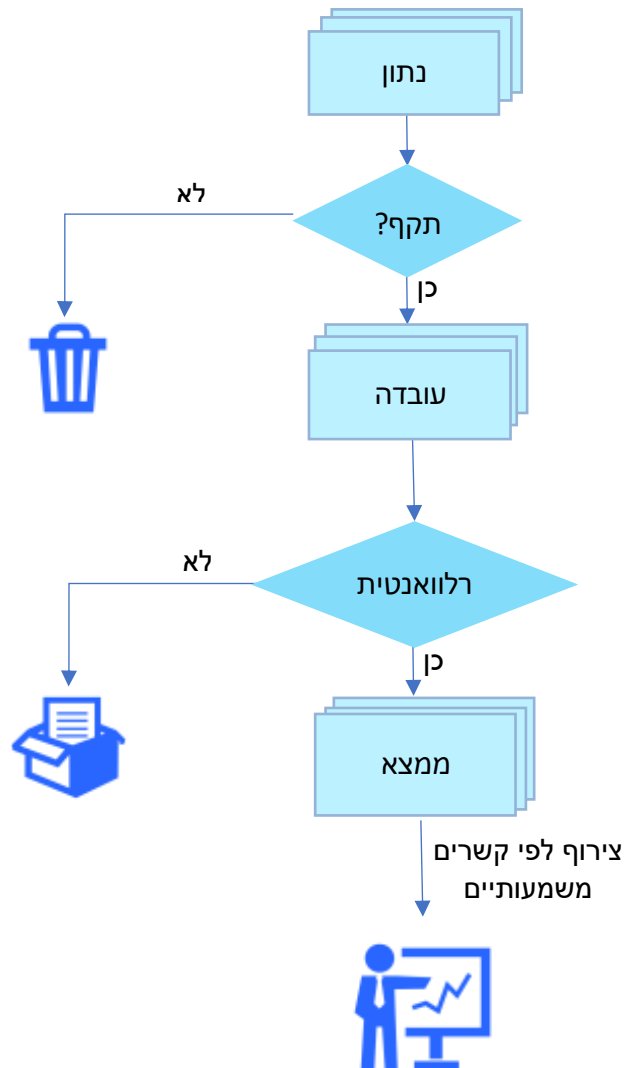
תחקור התרגיל מתחיל, למעשה, עוד בזמן התרחשותו של התרגיל. השלב הראשון שלו הוא איסוף של מירב המידע שהצטבר לאורך התרגיל ותייעודו על ידי המתורגלים. בתוך אלה יש למנות, למשל, רשומות המיוצרות על ידי מערכות אוטומטיות או רשתות תקשורת, וכן רשומות כתובות, כגון יומני מבצעים, טופסי דיווח שונים, וכיו"ב. מובן מאליו, שתיעוד המידע הזה הוא תנאי הכרחי לקיום תהליך הפקת הלקחים מהתרגיל.³⁸ מטבע הדברים, המידע הגולמי שנאסף עשוי להכיל נתונים שגויים, ואחרים, שהינם נכונים, אך לא רלוואנטיים להפקת הלקחים. לפיכך, השלב הבא בתהליך התחקור הוא אימות הנתונים שנאספו. מה שהוכר כשגוי (או אפילו לא בר-אימות באופן סביר) - מנופה מתוך המידע שנאסף. הנתונים שנותרים בתהליך אחרי שלב זה מוגדרים כ**עובדות**. בשלב הבא, נערך בירור אילו מהעובדות רלוואנטיות להפקת הלקחים. מי מהן שאינן כאלה, מנופות ונשמרות במאגר נפרד, שכן, הן עשויות להימצא רלוואנטיות בהקשרים אחרים - תרגיליים או אמיתיים, עכשוויים או עתידיים. שאר העובדות שנותרו לאחר שלב זה מוגדרות כ**ממצאים**. בשלב האחרון והמכריע של תהליך התחקור, על המתחקרים לצרף את הממצאים אלה-לאלה לכדי תיאור קונסיסטנטי, וככל האפשר שלם ומלא, של מהלכיהם לאורך התרגיל. הצירוף נעשה על בסיס זיהוי של קשרים בין הממצאים (בעיקר

³⁸ בעניין זה יש לזכור, שמימוש התנאי הזה תלוי, בעיקרו של דבר, בתרבות הארגונית של המתורגלים: קיומה של אסטרטגיה כלל-ארגונית (מהו ייעודו של הארגון? מהן מטרותיו? מהן משימותיו הקבועות? מהי הגישה הכללית למימושן? כיצד מבטיחים את שימור יכולותיו הקיימות של הארגון? באילו פעולות יש לנקוט כדי להבטיח את הרלוואנטיות של הארגון לקהל היעד שלו? וכו'); קיומן של תפיסות הפעלה ארגוניות; קיומם של נהלי עבודה פנים-יחידתיים, חוצי-ארגון ובין-ארגוניים; וכיו"ב. עניין זה מעמיד את האפקטיביות של פעילות התרגול הארגונית בהקשר רחב יותר, כמובן.

מהסוג של "סיבה-מסובב": למשל, "ממצא X גרם להתרחשות ממצא Y". סוג נוסף של קשר הוא התרחשות במקביל של ממצאים שונים, או התרחשות בזמנים שונים של ממצאים זהים. למשל: "ממצא X התרחש במועד מסויים בנכס סייבר מסויים של הארגון, וכעבור שעותיים, ממצא Y, הזזה לו במהותו ובסממניו, התרחש בנכס סייבר אחר שלו". העובדה שמרחב הסייבר הארגוני הוא, בהגדרתו, מצרף של נכסים, מקלה על יצירת קשרים משמעותיים בין הממצאים הנוגעים לנכסים אלה.

תרשים מס' 2 שלהלן מתאר את תהליך התחקור מתחילתו ועד סופו.

יש לשאוף לכך שהתמונה המתקבלת מצירוף הממצאים זה-לזה תהיה מקובלת על כלל המשתתפים בתחקיר, שכן, הדבר מהווה מדד חשוב למידת המהימנות שלו. לפיכך, תוצר זה, שיכונה להלן בשם "התמונה התרגילית", צריך לקבל את אישורה של הסמכות הבכירה ביותר בתוך הארגון, שהשתתפה בתרגיל.³⁹



תרשים מס' 2: תהליך התחקור

³⁹ מהותו של אישור זה היא הצהרה רשמית על כך שהתמונה התרגילית היא תיאור נאמן של מה שהתרחש לאורך התרגיל. אין הכוונה כאן לבדיקה של התמונה התרגילית ושל תהליך התחקור לפרטיהם.

הפקת הלקחים

אחת שהתמונה התרגילית סוכמה ואושרה, ניתן לבחון את אופן היווצרותה לאורך התרגיל, על פי מדדים נתונים מראש (כנזכר בתחילת המדריך). על הפרק עומד, למעשה, צמד שאלות מרכזי: מדוע מה שקרה - קרה כך, והאם (בנסיבות הנתונות) נכון היה שיקרה אחרת? התשובות לשאלות אלה הן התובנות שישמשו בסיס להפקת הלקחים מן התרגיל. לא כל מה שעולה מתוך כך הוא בהכרח חדש - אולם, גם תובנות ידועות זה מכבר הן חשובות, שכן כל חשיפה שלהן מגדילה את תוקפם של הדברים האמורים בהן, ומסייעת לביסוס מוסכמות שעליהן יישען תפקודו העתידי של הארגון. בהמשך ישיר לכך, תובנות חדשות הן דבר שיש לברך עליו - אך גם לנהוג בו במידה של זהירות: ייתכן שהנסיבות שמהן הן נובעות היו בבחינת צירוף-מקרים יוצא דופן, למשל. יתירה מכך, יש לשוב ולהזכיר שמדובר כאן בתרגיל, כך שיתכן שאלמלא הסימולציה התרגילית, צירוף המקרים הזה לא היה קורה כלל. בגוף המדריך צויינה חשיבותו של הכישלון ככלי למידה. בהקשר הנדון כאן, אפוא, יש לציין כי את הצלחותיהם של המתורגלים חשוב לתחקר לא פחות מאשר את כישלונותיהם.

כשם שאישרה את התמונה התרגילית, כך על הנהלת הארגון לאשר גם את רשימת התובנות שגובשו על בסיסה. תובנה שאושרה מוגדרת כ**לקח**, וככזו, יש לה מעמד מחייב בארגון. להלן רשימה של המרכיבים העיקריים של המוכנות הארגונית שהלקחים עשויים לגעת בהם:

- תכניות העבודה והנהלים של הארגון.
- המבנה הארגוני של גופים בארגון - או של הארגון בכללו.
- תהליכי הניהול של הארגון (תהליכי "זרימת המידע" בארגון, ומנגנוני קבלת ההחלטות המבוססים עליהם).
- משאבים ארגוניים (כוח אדם; מערכות תקשוב - חומרה ותוכנה; מערכות אחרות; אמצעים לוגיסטיים; תקציבים - היקף וחלוקה; וכיו"ב).

בשפה המקובלת בארגונים רבים נהוג להבחין בין "לקח לשימור" (תובנה המצביעה על נקודת חוזק שראוי לשמרה) לבין "לקח לשיפור" (תובנה אודות נקודת כשל, חולשה או חסר המציינים תיקון). לפעולת האישור הזו יש חשיבות רבה, שכן, לקח אינו רק מלמד דבר מה אודות הארגון ותפקודו - הוא טומן בתוכו גם חובת עשייה הנובעת מכך. במילים אחרות, לקח שהופק הוא חסר משמעות, אלא אם כן הוא גם **יושם**. לפיכך, יש "לתרגם" את הלקחים שהופקו למשימות, ולשלב את אלה בתכנית העבודה של הארגון. כיוון שלמידה היא תהליך מעגלי, אופן יישומם של הלקחים ותוצאותיו בפועל צריכים לשוב ולהיבחן בתרגילים העתידיים של הארגון, שגם הם, כמובן, נועדו להפקת לקחים ויישומם - וחוזר חלילה.

תיעוד התהליך

- עם סיום תהליך הפקת הלקחים, תפרסם יחידת התרגילים הארגונית דוח להנהלת הארגון, לכלל המתורגלים, למנהלת התרגיל ולכלל גורם אחר הנוגע בדבר, ובו:
- מתווה התרגיל.



- מהלך התרגיל בפועל - נקודות עיקריות הראויות לציון.
- לקחי התרגיל: מרכיב זה יכלול קביעה של הגוף האחראי ליישום כל לקח. יודגש, שלא מדובר כאן בתכניות העבודה ליישום הלקחים - אלה יוכנו ויפורסמו על ידי הגופים האחראים ליישומם.
- לקחי המנהלת: תובנות אודות התרגיל עצמו (תיק התרגיל ואופן יישומו בפועל), ופעולות שבכוונת יחידת התרגילים הארגונית לנקוט לאורן לקראת התרגילים העתידיים של הארגון.



««« נספח א': קווים מנחים לבניית מתווה של תרגיל סייבר

כללי

בהתאם למה שהוסבר בתחילת הדברים, גוף המדריך התמקד בהמשגה של עולם התרגול, תוך מתן דגשים עיקריים על תרגול בממד ובמרחב הסייבר. על הבסיס הזה מונחים ארבעת הנספחים שלהלן, המוקדשים - כל אחד בתחומו - לפעולות קונקרטיים שעל יחידת התרגילים הארגונית והמנהלת של כל תרגיל לבצע לצורך הבנייה והניהול של תרגילי סייבר. בהתאם לזאת, הם מתמקדים בסוגיות נבחרות, המחייבות העמקה ופירוט נוסף. לפיכך, מומלץ לקרוא אותם רק לאחר קריאת גוף המדריך. נספח א' שלהלן מתמקד בתהליך הבנייה של המתווה של תרגיל סייבר.

מתווה התרגיל - ותכנית התרגילים הארגונית

כפי שכבר הוסבר, מתווי התרגילים הכלולים בתכנית העבודה השנתית של הארגון מהווים חלק בלתי נפרד מתכנית התרגילים השנתית שלו, ולפיכך, יש לבנותם כחלק מבנייתה של תכנית זו. הקפדה על כך לא רק תאפשר למתורגלים להיערך מבעוד מועד לכל תרגיל ותרגיל - היא גם תספק להם עוגנים לאורך שנת העבודה, שלאורם יוכלו לבחון את כשירותיהם ומוכנותם לאירועי אמת אפשריים. לפיכך, על יחידת התרגילים הארגונית לבנות את תכנית התרגילים השנתית באופן שישקף בצורה הנאמנה ביותר את יעדי הכשירות והמוכנות של הנהלת הארגון לאותה שנת עבודה. בבניית התכנית השנתית יש לקחת בחשבון את קבועי הזמן האופייניים להכנת טיפוס התרגילים השונים. תרגיל מהטיפוס העיוני מצריך תקופת הכנה בת חודש עד חודשיים, בדרך כלל. תרגיל מהטיפוס התפקודי מחייב הכנה ארוכה יותר - בדרך כלל, מדובר בשלושה עד חמישה חודשים. עניין נוסף שיש להתחשב בו כשקובעים את תמהיל התרגילים העיוניים והמעשיים לאורך השנה הוא העובדה, שתרגול עיוני עשוי תמיד לשמש בסיס לתרגול מעשי.

תהליך בניית המתווה

בהמשך לכתוב לעיל, תהליך בניית המתווה כולל את המשימות הבאות:

- קביעת מושאי הלמידה מן התרגיל (מטרה, הרכב המתורגלים, מטרת משנה ונושאי תרגול).
- קביעת מתכונת התרגול.
- קביעת ציר הזמן שלפיו יתקיים תהליך ההיערכות של המנהלת ושל המתורגלים לקראת התרגיל (לרבות קביעת תאריכים קונקרטיים לביצוע אבני הדרך שמהן בנוי התהליך).
- קביעת המשאבים הנחוצים לתכנון התרגיל ולעריכתו (תקציב, כוח אדם, מקום עריכתו הפיסי של התרגיל, אמצעים טכנולוגיים ולוגיסטיים, וכיו"ב). יודגש, שגיוס המשאבים האלה בפועל הוא חלק בלתי נפרד מאחריותה הקבועה של יחידת התרגילים הארגונית, והעיסוק בו, לפיכך, צריך להיות מתוזמן קלנדרי במסגרת תכנית העבודה הכוללת שלה.

קביעת מטרת התרגיל

הבנייה של מתווה התרגיל מתחילה בקביעת מטרת התרגיל. המטרה צריכה להיות מנוסחת במונחים הנוגעים ישירות למרחב הסייבר הארגוני, וליתר דיוק - בראייה של שיפור וקידום החוסן של הארגון בסייבר. אולם, כמוסבר כבר, מרחב הסייבר הארגוני אינו עומד לעצמו, ולכן, ככלל, נדרש להתייחס בעניין זה גם לרציפות התפקוד הארגונית ולהמשכיות העסקית שלו. היוצא-מן-הכלל עשוי לחול במקרה של תרגיל ברמה הטכנו-טקטית (כגון כזה שמיועד לגורמים טכנולוגיים ותפעוליים נמוכי-דרג הממונים על הגנת הסייבר של הארגון). כמובן, קביעת המטרה צריכה להתבסס על כלל המידע הרלוואנטי שנצבר בארגון עד לאותו רגע - לרבות לקחי תרגילים קודמים.

להלן המטרות האופייניות שאותן נהוג - ומומלץ - לקבוע עבור תרגיל סייבר:

- (1) העלאת מודעות ההנהלה של הארגון לחשיבות ההגנה עליו בסייבר.
- (2) העלאת מודעות העובדים בארגון לחשיבות ההגנה בסייבר.
- (3) חשיפת פערים בחוסן הארגוני בסייבר על היבטיו השונים (חולשות ופגיעויות בארכיטקטורה של מערכות התקשוב של הארגון; התלות שלו בשרשרות אספקה; תהליכי ההגנה בסייבר הקבועים או נהוגים בו; האפקטיביות והיעילות של מנגנוני ההגנה הטכניים הקיימים בו, וכו').
- (4) חשיפת פערים בכשירות ובמוכנות של כוח האדם האחראי להגנה בסייבר של הארגון.
- (5) חשיפת פערים בכשירות ובמוכנות של מרכיבים אחרים בארגון (בעלי תפקיד יחידים כמו-גם מסגרות ארגוניות).

כבר באופן ניסוחה, המטרה שנקבעה מצביעה על הרמה שבה התרגיל ייערך (אסטרטגית, תפעולית או טכנו-טקטית), ומכאן נגזרת גם השפעתה המכרעת על הרכב המתורגלים. למעשה, מטרות (1) ו-(2) המובאות לעיל קובעות בניסוחן (הגם שלא באופן ספציפי) גם את הרכב המתורגלים. שתיהן גם-יחד מכוונות לתרגיל ברמה האסטרטגית. מטרה (3) שלעיל מכוונת, בעיקרו של דבר, לרמה התפעולית, אך ניתן לכוונה גם לרמה הטקטית. במקרה הראשון, נקודת המבט של המנהלת תהיה מערכתית, ומכאן, שעיקר המתורגלים יהיו מנהלים בכירים וזוטרים האחראים לביצוע תהליכי ההגנה בסייבר בארגון. במקרה השני, מדובר בתרגול של מרכיבים נבחרים מתוך הארגון, או אף של מרכיב יחיד, ומכאן, שהמתורגלים יהיו הן המנהלים והן חלק, לפחות, מן העובדים הנוגעים בדבר. מטרות (4) ו-(5) הן טקטיות, ואפילו טכנו-טקטיות, ולפיכך, המתורגלים במקרה הזה יהיו בעיקר עובדים בתחומי התמחות שונים, כאשר תחום ההתמחות של העובד חשוב הרבה יותר מרמת בכירותו.

כאן המקום להזכיר, כי לא זו בלבד שנכון להסתפק במטרת תרגול אחת ויחידה - רצוי מאוד גם להתמקד בתרגול של רמה ארגונית אחת ויחידה. לכאורה, מתבקש לנצל את עצם עריכת התרגיל לטיפול במספר מטרות, או, לפחות, לתרגול ביותר מרמה ארגונית אחת - בעיקר משיקולים של יעילות וחסכון במשאבים. אולם, קרוב לוודאי שהניסיון לממש זאת יחבל באפקטיביות של התרגיל, בבחינת "תפסת מרובה - לא תפסת". ההסבר לכך נעוץ בעובדה שהפעילות של כל רמה ארגונית מבוצעת, במידה רבה, מתוך "היגיון פנימי" שייחודי לה - אינטרסים אסטרטגיים לא זו בלבד שהם שונים מאלה הטקטיים, למשל; לעיתים מזומנות, הם אף עשויים לסתור זה את זה. ומאחר וכל רמה ארגונית רואה,

בצדק, חובה לעצמה לקדם את האינטרסים שלאורם היא פועלת, תרגול של כל רמה יוצר, למעשה, תרגיל נפרד. אין בכל זה כדי לסתור מוסכמה אחרת וחשובה לא פחות: נכון יהיה שהתרגול של כל רמה ארגונית גם יאתגר אותה בהתמודדות עם ניגודי אינטרסים בינה לבין הרמות הארגוניות האחרות. אלא שלשם כך לא נדרש לתרגל את הרמות האחרות - די בכך שהן ידומו על ידי מנהלת התרגיל באמצעות תפקידנים מתאימים.

קביעת מתכונת התרגול

משנקבעו מטרת התרגיל והרכב המתורגלים, ניתן כבר לקבוע גם את מטרות המשנה ונושאי התרגול. אבן הדרך הבאה בתהליך הבנייה של המתווה היא גם המעבר מן ה"מה" ("מהי תכלית התרגיל?") ל"איך" ("איך תכלית זו תמומש?"). בהמשך לדיון בגוף המדריך באופן הקביעה של מתכונת התרגול, המתכונת המתאימה ביותר לתרגול לאור מטרה (1) דלעיל היא **תרגיל שולחני** (או **משחק ארגוני**). לעומת זאת, המתכונת המתאימה ביותר למטרות (2) ו-(4) היא **תרגיל תפעולי**. מטרה (3) היא, מעצם הגדרתה, רחבה למדי, ולכן נדרשת הגדרה מדוקדקת ככל הניתן של מטרות המשנה ושל נושאי התרגול הנגזרים ממנה כדי לבחור במתכונת התרגול המתאימה ביותר למימושה. ככלל, אם מימוש מטרת התרגיל יחייב הפעלה מערכתית רחבה של הארגון, מומלץ יהיה לערוך תרגיל **תפעולי**; לעומת זאת, אם התרגול יתמקד רק במרכיבים מסויימים של הפעילות הכלל-ארגונית, בהיבטים מסויימים שלה, או בחתכים מסויימים של המערכת הארגונית השלמה, אזי מומלץ יהיה לערוך תרגול **שולחני** או **משחק ארגוני**.

יצוין, שמתכונת התרגול שתיבנה בפועל במסגרת המתווה עשויה ללבוש צורות קונקרטיזיות רבות - מתכונות התרגול, כפי שהוגדרו בגוף המדריך (ובמיוחד - התרגיל השולחני והמשחק הארגוני), הן יותר בבחינת "טיפוסים מייצגים" ראשיים, שכל אחד מהם עשוי להתגלם פיסית בשלל צורות. הגורם המכריע בהשפעתו על עיצוב מתכונת התרגול שתשמש בפועל את התרגיל הוא המכלול של אותם המאפיינים המייחדים של הארגון, שיש להם נגיעה למטרת התרגיל, ובאופן ספציפי - המיקום והמיצוב של כל אחד מהמתורגלים בתוך המבנה הארגוני.

להלן מקרה מייצג אחד להמחשת הכתוב לעיל:

קונצרן X השייך לתעשייה הכימית הינו הבעלים של מספר מפעלי ייצור אשר צורכים - וגם מייצרים - שורה של חומרים מסוכנים. לאור זאת, קבע הקונצרן תכנית להיערכות למצבי משבר ולהתמודדות עם מצב משברי - בין אם כזה המסתמן באופק הקרוב, או כזה שכבר מתחולל. התכנית מקיפה הן את ההנהלה הראשית של הקונצרן והן את כל המפעלים השייכים לו. בעקבות בחינה מקיפה של התכנית, בוצעו בה שינויים מהותיים, ולפיכך, החליטה ההנהלה הראשית לבחון את מידת האפקטיביות שלהם ואת משמעויות אימוצם בפועל. לצורך כך, בנתה יחידת התרגילים של הקונצרן תרגיל עבור ההנהלה הראשית שלו ועבור ההנהלות של כל מפעלי הייצור שלו. לאור המיקוד של התרגיל, הובן כי נכון שהתרגול יהיה עיוני, ובהתאם לכך, נקבע כי התרגיל ייערך במתכונת שולחנית. בהתחשב במבנה הארגוני של הקונצרן, חולקו המתורגלים לצוותים על פי שיוכם (מפעלים, הנהלה ראשית), ומהלך התרגיל נבנה על פי המתואר בטבלה שלהלן.



לוח הזמנים של התרגיל השולחני לקונצ'ן X

מיקום	מופע	שעה
אולם מליאה	התכנסות במליאה: פתיחה, תדריך כללי והזרמת ידיעות ראשונה	09:00-09:30
חדרי צוות	עבודה בצוותים: הזרמת ידיעות שנייה, מפוצלת צוותית	09:30-10:15
אולם מליאה	התכנסות במליאה: חיתוך מצב, דיון חופשי והזרמת ידיעות שלישית	10:15-11:15
חדרי צוות	עבודה בצוותים: הזרמת ידיעות רביעית, מפוצלת צוותית	11:15-12:00
אולם מליאה	התכנסות במליאה: חיתוך מצב, דיון חופשי וסיכום התרגיל	12:00-13:00
אולם מליאה	תחקיר ראשוני	13:00-14:00

כפי שניתן לראות לעיל, יחידת התרגילים בחרה לממש את התרגיל השולחני על ידי ייצוג כל אחת מההנהלות שבקונצ'ן באמצעות צוות של מנהלים שייבחר מתוכה. לכל צוות ניתנה האפשרות להתכנס בתוך עצמו כדי להתמודד עם ההתפתחויות של התרחיש. נוסף על כך קבעה יחידת התרגילים גם כללים המסדירים חילופי מידע בין הצוותים לבין עצמם במהלך העבודה בפורום הצוותי. יחד עם זאת, נקבעה גם מסגרת המאפשרת חיתוכי מצב ברמה של כלל הקונצ'ן.

הגם שהאופן שבו עוצבה מתכונת התרגול המתוארת לעיל לא הפך אותה משולחנית לתפעולית, הוא בכל זאת העניק להתנהלות של התרגיל אופי דינאמי יותר, והודות לכך, שיווה לתרגיל צביון קרוב יותר, במידה מסויימת, למצב העניינים בחיים האמיתיים. כל זאת, כאמור, מבלי לחרוג מן המסגרת הכללית של תרגול במתכונת שולחנית, ויעידו על כך המִשְׁך הכולל של התרגיל, היקף המתורגלים והרכבם, והאופי האינטימי, יחסית, של האירוע בכללותו.

אישור מתווה התרגיל - ופרסומו

עם סיום בנייתו של מתווה התרגיל (הכולל, יש להזכיר, גם את הכנתו של המחווון התרגילי), נדרש לאשרו אצל הרמה הממונה המתאימה. ככלל, רצוי שהדרג הארגוני של הגורם המאשר יהיה אחד מעל זה של הגורם המתורגל הבכיר ביותר - או זהה לו, בהעדר אפשרות שכזו. פעולה זו נועדה, בראש ובראשונה, להשיג את גיבוייה ותמיכתה של הרמה הממונה בתרגיל, ואחת שכך, לתאם ציפיות איתה באשר לתכליתו של התרגיל, ולהפוך אותה לשותפה לכל דבר למאמץ הכולל המושקע בהכנת התרגיל ובעריכתו.

משאושר המתווה, יש לפרסמו רשמית, על מנת להביאו לידיעתם של הנהלת הארגון, של המתורגלים ושל כל גורם אחר השותף להכנת התרגיל ולעריכתו. בתוך כך, יש להקפיד שהמידע שיפורסם לא יכלול פרטים שאמורים להיות נסתרים מידיעתם של המתורגלים. הכוונה היא, בעיקר, לקובץ הידיעות התרגיליות. כמו כן, אין לכלול בפרסום את סיפור הרקע של התרגיל (במקרה שהוחלט להכין כזה) - את סיפור הרקע יש להפיץ למתורגלים זמן קצר לפני מועד עריכתו של התרגיל (כשבוע).



פרסום חוזר של מתווה התרגיל

אומנם, מתוויהם של התרגילים הכלולים בתכנית העבודה השנתית של הארגון מתפרסמים בקרב עובדי הארגון כחלק מפרסומה של תכנית העבודה הכוללת שלו, ולקראת תחילתה של שנת העבודה המדוברת. אולם, כחודש ימים לפני כל תרגיל, על מנהלת התרגיל להפיץ את המתווה הספציפי שלו למתורגלים ולכל גורם רלוואנטי אחר. הדבר נועד להבטיח, שכל הגורמים האלה יהיו מודעים לתרגיל הממשמש ובא, וכך, יוכלו לפתוח בהכנה נאותה לקראתו. הגם שהמתווה הוכן, כאמור, כבר לפני תחילתה של שנת העבודה, נקודת הזמן הזו מספקת הזדמנות עבור הארגון לבחון אותו שוב, ולוודא שהוא אכן משקף נאמנה את ציפיותיו מן התרגיל.

נספח ב': קווים מנחים לבניית תרחיש של תרגיל סייבר

כללי

מן הבחינה של עיתוי העשייה, הפעילות המתוארת בנספח א' מתרחשת לקראת פתיחתה של שנת עבודה חדשה של הארגון, ומבוצעת על ידי יחידת התרגילים שלו. לעומת זאת, הדברים המתוארים להלן מתרחשים כולם לקראת מועד עריכתו של כל תרגיל כשלעצמו, ומבוצעים על ידי מנהלת התרגיל, שהינה, כאמור, גוף זמני וייעודי שהוקם אד-הוק על בסיס המבנה הקבוע של יחידת התרגילים הארגונית.

מנגנון הבנייה של התרחיש

המתורגלים פועלים כבעלי תפקיד, המבצעים משימות אד-הוק, הנגזרות מנושאי התרגול, וכל זאת, על מנת להשיג הישגים נדרשים לאור היעדים של הארגון. הדינמיקה הזו מיושמת באמצעות תהליכי העבודה שהוגדרו בארגון לצורך זה.

פעולות התקיפה הנכללות בתרחיש מכוונות לאתגר את הדינמיקה הזו, על ידי פגיעה (מתודית) בנקודות תורפה המצויות בתהליכי העבודה הארגוניים הנוגעים בדבר. מאחורי נקודות התורפה האלה מצויים, למעשה, נכסי סייבר של הארגון (כמו, למשל, בקר ממוחשב המותקן בתשתית הייצור של הארגון, או מרכיב תוכנה המותקן בתשתית ה-IT שלו), שכל אחד מהם לוקה בחולשה (Vulnerability) כלשהי.

מומלץ, שהחולשות (Vulnerabilities) האלה יהיו מוכרות - או דומות לכאלה שהינן מוכרות - במרחב הסייבר⁴⁰. הדבר יגביר את אמינותו של התרחיש בעיני המתורגלים. מכל מקום, חשוב שהחולשות האלה יהיו סבירות. בהקשר זה, חשוב לחדד את הדרישה שהתרחיש יהיה מציאותי, מתקבל על הדעת ומאתגר: אין כל מניעה לכלול בתרחיש תקיפת סייבר שהארגון העריך את סיכוייה להתממש כנמוכים מאוד - אך העריך את פוטנציאל הנזק שלה כגבוה. יתירה מזאת - אין כל מניעה להשתמש בתקיפת סייבר, שלפחות על פי הפרסומים הידועים בעולם, ועד למועד בניית התרחיש, טרם נודעה כמותה אפילו בתור איום.⁴¹ כל שנדרש מן המנהלת בעניין זה הוא לספק בסיס הגיוני נאות לייזומה ולביצועה של תקיפה שכזו (כוונות ויכולות של תוקף, והיתכנות למימוש וקטור התקיפה). אחרי הכל, יש לזכור שמדובר בתרגיל ולא בניסוי או בדיון טכנולוגי.

מאחר שמדובר בתרגיל סייבר, התהליכים הארגוניים הנוגעים בדבר מבוססים במידה משמעותית על תשתיות התקשוב הארגוניות, או, לחליפין, על תשתיות תקשוב המקשרות בין הארגון המתורגל לארגונים אחרים, המצויים בשרשרת האספקה שלו. לפיכך, פעולות התקיפה צריכות לפגוע - או לאיים בפגיעה - במרכיבים מסויימים של

⁴⁰ מוזכר, שנקודות תורפה אלה זווה מבעוד מועד, ונבחרו כמוקד עניין תרגילי, במסגרת קביעת מטרות המשנה של התרגיל ונושאי התרגול. כמו כן חשוב להדגיש, כי לא מדובר בהכרח בחולשות מובנות בחומרה או בתוכנה, אלא גם בכאלה הנבעות מהגדרה או מניהול לקויים של נכסי הסייבר של הארגון (כמו, למשל, מדיניות הרשאות לקוייה של המשתמשים בארגון, או קונפיגורציה לקוייה של אמצעי הגנת סייבר המותקנים בארגון).

⁴¹ בהקשר זה ראוי להזכיר את המושג "ברבור שחור" (כפי שהוא מוגדר על ידי נאסים טאלב). מדובר בתופעה נדירה בעלת השפעה רבה, שלכאורה לא ניתנת לניבוי, אך ניתן להעריך שתתרחש בזמן כלשהו. אין כל מניעה להכניס "ברבור שחור" לתרחיש, ובלבד שישולב באורח משכנע במרקם ההתרחשויות הכולל.

תשתיות אלה. כמו במצב האמת, פגיעות אלה אמורות לגרום לנזקים מסויימים לתהליכים הללו. באופן כללי, מדובר באפקטים של שיבוש או השבתה. אלה, בתורם, אמורים לחולל נזק תפעולי לארגון.

ההשתלשלות הלוגית המתוארת לעיל מיושמת, הלכה למעשה, בסדר הפוך בעת שמנהלת התרגיל בונה כל תקיפת סייבר תרגילית - בדיוק כשם שתוקף בסייבר מתכנן תקיפת אמת שבכוונתו לבצע.⁴²

יוצא מכך, אם כן, שהצעד הראשון בתהליך תכנון התקיפה התרגילית הוא קביעה של הנזק התפעולי שייגרם לארגון. למעשה, על מנהלת התרגיל לעצב בראש ובראשונה את **תהליך ההידרדרות של התמונה התפעולית הכלל-ארגונית בתרגיל**. הדבר ישמש, כאמור, כנקודת המוצא לבניית כל תקיפת סייבר שתיכלל בתרחיש; אך, לא פחות חשוב מכך, הוא יסייע בידי המנהלת לגלגל את **משבר הסייבר** שאליו ייקלע הארגון כתוצאה ממה שקורה בתרחיש. קיימים שני טיפוסים של משבר סייבר, כשהבדלים ביניהם נעוצים הן באופן ההתרחשות שלהם על ציר הזמן, והן באופן שבו מתפתחת ההבנה של הארגון את מה שמתחולל בפועל:⁴³

- **הטיפוס המתפתח:** בתחילת התרגיל, לא ניכרים עדיין סימנים כלשהם לנזק תפעולי או עסקי לארגון (כלומר, על פניו נראה ש"העסקים כרגיל"). יחד עם זאת, ניכרים סממנים העשויים להעיד, לכל הפחות, על פעילות עויינת המאיימת על מרחב הסייבר הארגוני. מכאן, המצב הכללי הולך ומידרדר, ותקיפות סייבר כנגד הארגון כבר מתחילות להתחולל; כתוצאה מכך, מתחילים להיגרם גם נזקים תפעוליים או עסקיים מוחשיים לארגון.⁴⁴
- **הטיפוס הפתאומי:** כבר בתחילת התרגיל מתחילות להתחולל תקיפות סייבר (אם כי יכול להיות שהמתורגלים טרם אבחנו זאת), והתקיפות הללו גורמות לנזק תפעולי או עסקי מוחשי לארגון. מנקודה זו, המצב הכללי ממשיך להחמיר.

נקודות תורפה ארגוניות - ותקיפתן

התהליך המתואר לעיל מסתיים, אפוא, בקביעת נקודות התורפה במרחב הסייבר הארגוני שכלפיהן יהיו מכוונות תקיפות הסייבר שייכללו בתרחיש. להלן טיפוסים אופייניים של נקודות תורפה שכאלה:

- נכס סייבר שנפוץ בארגון.
- נכס סייבר שמהווה נקודת כשל יחידה (Single Point Of Failure - SPOF).
- נכס סייבר שמהווה חוליה חיונית בשרשרת ערך (Chain of Value) התומכת באחד מהתהליכים הארגוניים שנקבע לפגוע בהם במסגרת התרחיש.

⁴² מבחינת הלוגיקה שלו, תהליך הבנייה של התקיפה מבוסס על המודלים המוכרים והמקובלים של תקיפת סייבר (כמו, למשל, ה-Kill Chain של חברת לוקהיד-מרטין, המופיע ב"מודל הקרחון" הנדון בגוף המדריך).

⁴³ את הדבר הזה נהוג לכנות בשם "הבנה מצבית" (באנגלית: Situational Understanding). למעשה, ההבנה המצבית של כלל המתורגלים, ובמיוחד של אלה החברים בהנהלת הארגון, היא אחד מהנושאים המרכזיים לתחקור בעקבות התרגיל, שכן, היא מעידה על יכולתם של אלה לנהל משבר סייבר (לבנות תמונת מצב המשקפת את המציאות, לקבל על בסיסה החלטות נכונות, לנהל את מימושן בצורה אפקטיבית ויעילה, לבקר את התוצאה – וחוזר חלילה).

⁴⁴ מקרה מיוחד של משבר מתפתח הוא כזה, שבו עד לסוף התרגיל לא מתחוללות תקיפות סייבר בפועל. השימוש בו מתאים בעיקר לתרגול עיוני, ובמיוחד – למתכונת של משחק ארגוני.



• נכס סייבר התומך בשרשרת אספקה של הארגון. הצעד הבא הוא התאמה של תקיפות מול החולשות המצויות בנכסי הסייבר שנבחרו. משיקולים הנוגעים הן לאמינות התרחיש והן לשליטת המנהלת במהלך התרגיל, רצוי שמספר התקיפות הכולל בתרחיש יהיה בין אחת לחמש. בד-בבד, מומלץ שהתקיפות ייבנו במתאר שיאפשר להן להסתעף במהלך התרגיל, ואף להתחבר זו לזו. התוצר שיתקבל יהיה תרחיש **מורכב** (להבדיל מתרחיש **עמוס**). תרחיש מורכב יעמיד בפני המתורגלים אתגר משמעותי להעניק פרשנות נכונה לסממנים שיופיעו בידיעות התרגיליות, על מנת לבנות תמונת מצב שתשקף נאמנה את המציאות התרגילית. אתגר לא פחות משמעותי שיעמוד בפניהם הוא הניהול המבצעי של ההתמודדות עם התקיפות. גם כשתמונת המצב נכונה ומלאה, המצב עצמו צפוי להציב בפני המתורגלים דילמות באשר לדרכי הפעולה שבהן נכון יהיה לנקוט בעניינו. במילים אחרות, תרחיש מורכב ישרת נאמנה את הצורך לאתגר את המתורגלים בשני מישורי הפעילות הארגונית: קיום ושימור הרציפות של התהליכים הארגוניים הקריטיים, בד-בבד עם קיום ושימור של מרחב סייבר נקי מתקיפות, המאפשר אותם ותומך בהם.

”רעש” תרגילי

כפי שכבר הוסבר בגוף המדריך, כדי להבטיח את אמינותו של התרחיש ואת האפקטיביות של התרגיל, יש לשלב את תקיפות הסייבר התרגיליות עם אירועי ”רעש”, כשהכוונה בזה היא לכל התרחשות במרחב הסייבר הארגוני או בהקשר אליו, שאינה תקיפת סייבר או תולדה שלה. בכלל זה יש למנות תקלות טכניות ותפעוליות, וכן חיוויים שגויים של מחוונים שונים (בעיקר בתשתיות ובמערכות ייצור, אך גם בתשתית ובמערכות IT). אירועי הרעש צריכים, כמובן, לשאת צביון אמין, ולכן, עליהם להיות לקוחים מעולמות התוכן של המתורגלים ומההוויה התפקודית שלהם. מעבר לכך, חשוב שהסממנים שיעידו עליהם יהיו דומים - או אף זהים - לסממנים המעידים על תקיפות הסייבר הכלולות בתרחיש. לבסוף, למרות שהם בחזקת ”טפל”, בעוד שתקיפות הסייבר הן-הן ה”עיקר”, חשוב לבנותם באופן שיש בו כדי להניע את המתורגלים לפעול בעניינם כאילו היו תקיפות של ממש. כל אלה יסייעו לאתגר את המתורגלים הן בניתוח הסממנים (אותה פעולה המכונה triage) ובבניית תמונת המצב התרגילית, והן בניהול התגובה המבצעית שלהם לאור מצב העניינים. יחד עם זאת יש לזכור, שלאירועי רעש אין ערך משל עצמם. אשר על כן, יש להקפיד שהמינון שלהם בתרחיש לא יהיה מופרז. לסיום הדיון בסוגיה זו, הנה דוגמה לאירוע רעש בעולם מערכות ה-IT, המציף את המתח המובנה השורר בין המישור התפעולי למישור התקשובי בארגון:

במסגרת התרגול של רשת קמעונאית גדולה, בנתה המנהלת אירוע רעש שבו, במהלך עדכון מחירו של מוצר מסויים, התבצעה בשוגג הזנה של הספרה ”אפס” במקום ספרה אחרת במסד הנתונים של הרשת. המוצר המדובר נמכר רק בחלק מסניפי הרשת, ובהתאם לכך, העדכון הזה הופץ רק אליהם. או-אז, מסופי המכירה (Points Of Sale - POS) בסניפים אלה, ובהם בלבד, קרסו, עקב חלוקה באפס שביצע אלגוריתם מסויים במערכת ההפעלה שלהם. בעת הפצת הידיעות התרגיליות הנוגעות לאירוע הזה בתרגיל, כבר הייתה הרשת נתונה גם לתקיפות סייבר תרגיליות, והמתורגלים היו מודעים לכך היטב. בעקבות כל



זאת, הם עמדו בפני דילמה: האם להניח שמדובר בתקיפת סייבר נוספת, ובהתאם לזאת, אולי להשבית מרצון, למשל, את מסופי המכירה שבסניפים האחרים של הרשת - או להסתכן בכך שמדובר בתקלה, ולהניח למסופי המכירה שבסניפים האחרים להמשיך לפעול כסדרם?

”תקיפת סייבר” מול “אירוע סייבר” - וגזירת הידיעות התרגיליות מן התרחיש

הכותרת הארוכה של תת-הפרק שלהלן מכוונת להבדל בין הזווית שממנה רואה המנהלת את פרטי התרחיש, לבין זו שממנה רואים אותם המתורגלים. כמי שבנתה את התרחיש, המנהלת יודעת מדוע וכיצד התרחש בו כל דבר. לעומת זאת, המתורגלים רואים רק את הידיעות התרגיליות, שאינן מייצגות אלא את התוצאים (אפקטים) ה”גלויים לעין” של השתלשלות העניינים שהמנהלת בנתה. כך, למשל, בעוד שהמנהלת יודעת שהשתלשלות מסויימת אחת שכזו היא, למעשה, אירוע רעש (ולא תקיפת סייבר), המתורגלים עשויים לפרש את סממניה כאילו מדובר באירוע סייבר. השוני בין שתי נקודות המבט האלה הוא מאפיין מהותי של פעולת התרגול, והוא משקף, בדרכו, את השוני המובנה בין ראיית התוקף לראיית המגן בסייבר. לאור זאת, כשגוזרים ידיעה תרגילית מן התרחיש, חשוב ביותר לוודא, שהמידע המועבר בה אכן משקף באופן הטוב ביותר את מה שצפוי שהמתורגלים היו יודעים, לו הדברים היו מתרחשים במציאות. להלן דוגמה להמחשת העניין:

במסגרת תרגול של מערך התחבורה הציבורית היבשתית, שבו השתתפו גם הגורמים הממשלתיים הנוגעים בדבר, בנתה המנהלת תקיפת סייבר של תשתית התשלום הדיגיטלית התומכת אותו. כתוצאה מכך, חדלו מערכות הסליקה באוטובוסים ובתחנות הרכבת לזהות את אמצעי התשלום הדיגיטלי שבידי הנוסעים, דבר שהביא, כמובן, לשיבושים חמורים בתפקודה של התחבורה הציבורית. על מנת לבנות את הידיעות התרגיליות הנגזרות מתקיפה זו, בחנה המנהלת את השתלשלות האירוע הזה: נהגי האוטובוסים והעובדים בתחנות הרכבת יהיו, מן הסתם, הראשונים להבחין בהתרחשות החריגה. במקביל, ציבור הנוסעים צפוי להפגין מורת רוח רבה מן המתרחש, ובעידן הנוכחי, הדבר ימצא חיש מהר הד נרחב ברשתות החברתיות. משם, הוא יגיע במהירות רבה גם לאמצעי התקשורת ההמוניים. בד-בבד, סביר כי מורת הרוח הזו תוביל לגילויים שונים של פגיעה בסדר הציבורי, כך שגם המשטרה תמצא עצמה מעורבת. תהליך הגזירה הזה, המבוסס על ההיגיון הפשוט של “דבר גורר דבר”, הוביל את המנהלת ליצירת ידיעות המכילות דיווחים מתאימים של נהגים למוקדי התפעול של חברות האוטובוסים, ידיעות מקבילות עבור תשתית הרכבות, וכן - ידיעות תקשורתיות המדווחות על השיבוש האמור לעיל, כמו-גם על הפרות הסדר והמהומה הכללית שהולכת ומתפשטת בקרב הציבור הרחב. על כך הוסיפה המנהלת ידיעה ובה פנייה של משטרת ישראל לגורמים הממשלתיים הנוגעים בדבר לבירור פרטי ההתרחשות ולאופן המשך הטיפול בה.



כפי שעולה מן הדוגמה הנ"ל, מקבץ הידיעות המדובר אינו יכול להעיד, כשלעצמו, על כך שמקור הבעיה שנוצרה הוא בתקיפת סייבר כנגד מערכת התשלומים הדיגיטלית, כך שעל המתורגלים מוטלת האחריות לחקור את המתרחש בעצמם על מנת לברר את העניין. כמובן, הדינמיקה המתוארת כאן היא בדיוק זו שהמנהלת ביקשה לחולל, דהיינו - הנעה של המתורגלים לפעול באופן מסויים, וזאת, תוך שימור הצביון המציאותי והאותנטי של ההתרחשות.

הגזירה של הידיעות התרגיליות מן התרחיש היא הצעד הראשון (מתוך שניים) במימוש מרכיב הסימולציה בתרגיל. צעד זה מבוצע, כמובן, לפני עריכת התרגיל. הצעד השני - ניהול תהליך העברת הידיעות למתורגלים - מתרחש במהלך התרגיל עצמו, ולמעשה, הוא מהווה את ליבת עיסוקה של המנהלת במסגרת הזו. עוד על כך - בנספח הבא.



««« נספח ג': קווים מנחים לעריכה של תרגיל סייבר שולחני ומשחק ארגוני בסייבר

כללי

השוני בין שיטת התרגול העיונית לזו המעשית ניכר באופן בולט בהבדל שבין אופני העריכה בפועל של תרגילים הנערכים על פי שתי שיטות אלה. לפיכך, נספח זה יעסוק בעריכה של תרגיל שולחני ומשחק ארגוני, וזה שלאחריו - בעריכת תרגיל תפעולי. הגם שהדברים המובאים להלן מכוונים לרמה הפראקטית, מגבלותיו המובנות של אורך היריעה של מדריך זה מחייבות להתמקד בנקודות עיקריות בלבד, ואין לראות בכתוב משום "מתכון" הניתן ליישום ישיר ומוכני.

מסגרת הזמן הכללית

אורכו הכולל של תרגיל שולחני לא צריך לעלות על חצי יום (לרוב, ניתן להסתפק בפרק זמן של שעה וחצי עד שלוש שעות). כמו כן, רצוי לערוך אותו בחלקו הראשון של היום.

סביבת התרגול

בתצורה ה"קלאסית" שלו, תרגיל שולחני נערך סביב שולחן אחד ויחיד. הכוונה בכך היא, שהמתורגלים ישובים אל השולחן הזה, כאשר חשוב להבטיח, כי כולם רואים זה את זה. מכאן, הנוהג לכנות תרגיל מהסוג הזה בשם "שולחן עגול". אבל השולחן אינו חייב להיות עגול, כמובן, ובכל מקרה, יש לו "נקודת קצה", או, יותר נכון, "ראש": מדובר במקום ישיבה המיועד ל**מנחה התרגיל** (עוד על כך - להלן).

הלכה למעשה, בשל המגבלות הכרוכות בצורת העריכה הפיסית של התרגיל, ייתכן מצב שבו לא יהיה מקום סביב השולחן **לכל** המתורגלים. הדבר קורה כאשר לפחות חלק מהפונקציות המתורגלות מיוצגות לא על ידי בעל תפקיד בודד, אלא על ידי צוות המונה בעלי תפקיד אחדים. במקרה שכזה, ניתן להציב מעגל נוסף של מקומות ישיבה ("המעגל השני"), שיקיף מבחוץ את השולחן הזה ואת מקומות הישיבה המסודרים ישירות סביבו ("המעגל הראשון"). או-אז, בעל התפקיד הבכיר (או המרכזי, מבחינת מטרות התרגיל ונושאו) בצוות יהיה זה שישב במעגל הראשון, וכל השאר יתמקמו במעגל השני, מאחוריו ובסמוך אליו.

המעגל השני נועד לשמש גם את חברי מנהלת התרגיל (מקובל שראש המנהלת יישב במעגל הראשון), לרבות תפקידנים ומשקיפים.

יודגש, שהשיח התרגילי אמור להתקיים, לפחות ברובו, בקרבת יושבי המעגל הראשון. לכן, כדי להבטיח את האפקטיביות והיעילות של השיח סביב השולחן, חשוב להקפיד, שמספרם הכולל של יושבי המעגל הראשון יהיה, לכל היותר, בין 20 ל-30. מספרם הכולל של המתורגלים עשוי להיות, אומנם, גבוה יותר, ובהתחשב בכך, נדרש להתאים את גודל האולם שבו נערך התרגיל למספרם הכולל של המשתתפים.

כפי שכבר הוסבר, עריכה של תרגיל שולחני מתאפיינת, ככלל, באחדות של הזמן והמרחב. לפיכך, מתכונת תרגול זו מתאימה במיוחד לכל מצב שבו, למשל, שיקולים של הרשאות חשיפה למידע, או תכתיבים הנובעים ממבנה ארגוני, אשר עשויים לחייב מידור



פנימי של המתורגלים אלה-מאלה, אינם בנמצא. לחליפין, מטרת התרגיל עשויות להיות כאלה, שעל מנת להשיגן, מתכנני התרגיל יבחרו "להפיל מחיצות" שכאלה במכוון. אולם, לעיתים נכון ונדרש לקיים מידור פנימי של המתורגלים לצורך עריכת התרגול. המקרה האופייני והשכיח הוא זה של משחק ארגוני. בנסיבות שכאלה, לא ניתן לערוך את התרגול במרחב אחד משותף, ולפיכך, המתורגלים נחלקים לצוותים, שכל אחד מהם ממוקם בחדר או באולם נפרד (או, לכל הפחות, בריחוק נאות משאר הצוותים). הואיל וכל צוות שכזה פועל בתנאים של אחדות זמן ומרחב, כל אשר נכתב לעיל בהקשר לכך תקף לגביו. יתר על כן, גם במשחק ארגוני יידרש, ככל הנראה, לכנס מדי פעם את כלל המתורגלים יחד במרחב אחד (מליאה). כינוס המליאה משמש בעיקר לצורך ביצוע "חיתוך מצב", המאפשר למתורגלים ולמנהלת להבין את תמונת המצב התרגילית הכוללת. כמובן, הסיכום של המשחק הארגוני והתחקיר הראשוני שלו יתבצעו גם הם במליאה.

ניהול התרגיל

כאמור, מקום הישיבה בראש השולחן מוקצה למנחה התרגיל. תפקידו - לנהל את השיח התרגילי, בעוד המנהלת מגלגלת את התרחיש באמצעות העברה של הידיעות התרגיליות ליושבי המעגל הראשון, ולסייע בכך בידה להשיג את מטרת התרגיל. המנחה עשוי להיות מתורגל בעצמו (ובמקרה הזה, לתפקיד הארגוני האמיתי שלו יש משמעות ניהולית ברורה בתרגיל); לחליפין, הוא עשוי להיות חבר מנהלת (אך בדרך כלל לא ראש המנהלת עצמו). ככזה, הוא עשוי להיות תפקידן, אך ייתכנו מקרים שבהם תפקידו יישא אופי ניהולי בלבד (כלומר, הוא לא יגלם שום תפקיד הלקוח מתוך הארגון ואשר יש לו זיקה ישירה ועניינית למטרות התרגיל ולנושאייו). המנחה צריך, אפוא:

- להיות בעל ניסיון ניהולי בסיסי, הכולל את המיומנות של הנחיית דיונים.
- להכיר את הארגון המתורגל.
- להניע את השיח התרגילי בהתאם למטרות התרגיל ונושאייו ועל פי ה"שעון התרגילי", וכל זאת, תוך שליטה בדינמיקה של הדיון.
- לשמור על תרבות דיון נאותה.

אם המנחה מתורגל בעצמו, אין הוא חשוף לתרחיש, וההיגיון המוביל את תפקודו נובע מהגדרת אחריותו הארגונית ומהאופן שבו מצופה ממנו לממשה לאור נסיבות התרחיש. במקרה הזה, מוטלת על המנהלת האחריות לוודא כל העת שפעולת המנחה אכן משרתת את ייעודה כנדרש. לעומת זאת, אם המנחה הוא חבר מנהלת, עליו להכיר את התהליכים והנהלים הארגוניים המופעלים בתרגיל (באופן מתודי, כמובן), וכיוון שהוא בקיא בפרטי התרחיש, הצורך שלו ביד מכוונת של המנהלת צפוי להיות קטן יותר. למען הסר ספק, ראש המנהלת לבדו הוא זה המוסמך לקבל את ההחלטות הקובעות לגבי תזמון התרגול (קביעת שעת תחילתו בפועל, קביעת הפסקות או ביטולן, האצה או האטה של קצב גלגול התרחיש, וקביעת שעת סיומו).

במשחק ארגוני, ימונה לכל צוות מתורגלים מנחה (לרבות מנחה עבור המליאה). במקרה הזה, אופייני ומקובל שהמנחה יהיה אחד מחברי הצוות, אולם, גם כאן, אין זה הכרחי. בשל המורכבות הניהולית הגדולה יותר הקיימת כאן, על המנהלת להשתמש בתצפיתנים שלה



לא רק על מנת לתעד את הפעילות הצוותית באופן שוטף, אלא גם כדי לסייע בידי המנהלת לנטר את פעילותם של כלל הצוותים ולכוון אותה לאור מטרות התרגיל.

הכנה טכנית ולוגיסטית של סביבת התרגול

בגוף המדריך הובאה כבר התייחסות לעניין זה, שנגעה בהיבטים הטכניים והלוגיסטיים המשותפים לתרגול העיוני והמעשי. להלן מובאים ההיבטים המיוחדים לתרגול העיוני:

- יש לסיים את הכנת מרחב התרגול ערב מועד עריכת התרגיל.
- מן הראוי להציב על גבי שולחן התרגיל ערכת כלי כתיבה אישית עבור כל אחד מיושבי המעגל הראשון (דפדפת או מחברת, ועט). הדבר יעודד אותם להעלות מחשבות על הכתב, ויסייע בכך לליבון הסוגיות שבהן עוסק התרגיל. יתר על כן, רשימותיהם של המתורגלים יוכלו לסייע בידם בביצוע התחקיר הראשוני והתחקיר הפנימי שיבוא בעקבותיו. ככלל, רשימותיו של מתורגל הינן קניינו האישי, וזכות הגישה לכתוב בהן שמורה לו בלבד. אם בחר מתורגל שלא לקחת עמו את רשימותיו בתום התרגיל, על המנהלת מוטלת האחריות לבער אותן.
- ביום עריכת התרגיל, מומלץ לצרף לאמצעים שהועמדו לרשותם של יושבי המעגל הראשון גם מסמכים המכילים מידע הנוגע לנושאי התרגול (תהליכי עבודה, נהלים, וכיו"ב). יש להקפיד לאסוף מסמכים אלה בתום התרגיל ולהחזירם למקום האחסון שלהם בארגון.
- מומלץ להציב על גבי שולחן התרגיל שילוט מזהה של יושבי המעגל הראשון (שם מלא, שיוך ארגוני ותואר תפקיד). הדבר יקל עליהם להתמקם סביב השולחן ולזהות זה-את-זה.
- כהשלמה לכך, חשוב לקיים בתחילתו של יום עריכת התרגיל הליך של רישום המשתתפים בו. כמו כן, יש לצייד כל אחד מהם בתג זיהוי אישי. הדבר לא רק יסייע למנהלת במעקב אחר הרכב המשתתפים בפועל, אלא גם במניעת כניסה של גורמים שאינם אמורים להשתתף בתרגיל אל מרחב התרגול. בהמשך לזה, ובוודאי במקרים שבהם מדובר בנושאי תרגול רגישים, יש להמשיך בקיום בקרה מתמדת של הנכנסים למרחב התרגול עד לסיום התרגיל.
- יש תועלת רבה בהצגת הידיעות התרגיליות על גבי צגים המותקנים במרחב התרגיל. תועלת זו עולה ככל שמספר המתורגלים גדול יותר. בכל מקרה, מומלץ להעביר ידנית לפחות ליושבי המעגל הראשון עותק מודפס של כל ידיעה שמוצגת, על מנת שיוכלו לשרטט לעצמם את רצף ההתפתחות של התרחיש.
- במקרה שמשך התרגיל אינו עולה על שעתיים, רצוי להימנע מקביעת הפסקות כלשהן במהלכו, כיוון שהדבר עשוי לפגוע במתח התרגילי ובדינמיקה הכללית שלו. בתרגיל ארוך יותר, מומלץ להסתפק בהפסקה אחת בלבד.

««« נספח ד': קווים מנחים לעריכה של תרגיל סייבר תפעולי

מסגרת הזמן הכללית

אורכו הכולל של תרגיל תפעולי עשוי לנוע בין יום אחד לימים אחדים. ככלל, הוא נמצא ביחס ישר הן להיקף הגורמים והגופים המתורגלים, והן לרמת המורכבות הארגונית של התרגיל.

סביבת התרגול

כאמור בגוף המדריך, חשיבות רבה נודעת לכך, שבסביבת התרגול מן הטיפוס התפעולי יבואו לידי ביטוי מירב המרכיבים של סביבת האמת. מעבר למרכיבים "רכים" כמו שיטות פעולה ונהלי עבודה, מדובר, למשל, גם באמצעי התקשורת שבהם משתמש הארגון בזמן אמת (ובדגש על מצבי משבר).

בתרגול תפעולי ברמה הטכנו-טקטית נשמרת, בדרך כלל, אֶחָדוֹת המקום: גם אם מדובר במספר צוותים המתורגלים במקביל, שכל אחד מהם ממוקם בחדר או אפילו במבנה נפרד, הרי שמרחבי התרגול האלה יהיו, קרוב לוודאי, סמוכים זה-לזה. כפי שכבר צויין, האפקטיביות של תרגיל מהסוג הזה תלויה במידה מכרעת בדימוי ראוי של תשתיות סייבר ארגוניות מטיפוסים שונים (בעולמות ה-IT וה-OT), כמו-גם של תקיפות סייבר מסוגים שונים המכוונות כלפיהן. שלא במפתיע, מדובר בתחום התמחות מקצועי ועתיר-משאבים, שהעיסוק בו מחייב תשתיות, אמצעים וכוח-אדם ייעודי, ואשר לרוב מוציא בפועל את התרגיל מתוך המרחב הפיסי של הארגון אל מתקנים חיצוניים שונים, המספקים שירות שכזה (ואכן, יש לא מעטים כאלה בארץ ובעולם).⁴⁵ מאפיין זה מבדיל את התרגול הטכנו-טקטי מזה שבשאר הרמות של הארגון, שכן, הוא כורך אותו בשיקולים לוגיסטיים וכלכליים בעלי משקל.⁴⁶ יחד עם זאת, במקרה המדובר כאן המרחק המעשי בין תרגיל לאימון הוא קטן למדי, כך שניתן לכרוך את צרכי התרגול של הארגון ברמה הזו בצרכי האימון שלו, ובאופן זה, לחסוך משאבים ניכרים.

כשמדובר בתרגיל תפעולי ברמה האופרטיבית והאסטרטגית של הארגון, אחדות המקום לרוב אינה מתקיימת, ולפיכך, בהכרח, המתורגלים עשויים להיות ממוקמים פיסית ואף גיאוגרפית בפיזור ניכר. כך, למשל, במקרה שמדובר בתרגיל תפעולי של מספר מפעלי ייצור המאוגדים תחת קונצרן אחד (שהנהלתו מתורגלת אף-היא), ייתכן כי התרגיל ייערך בעת ובעונה אחת באתרים הפרוסים על פני שטח נרחב של המדינה.

בשונה מתרגול עיוני, אין מגבלה קבועה מראש על מספר המתורגלים, והתנאי המגביל היחיד הקיים הוא יכולתה של המנהלת לשלוט במהלכי התרגיל, ובמקרה של תרגיל ברמה טכנו-טקטית - גם הקיבולת של תשתית הסימולציה התומכת את התרגול.

⁴⁵ תרגילים תפעוליים הנערכים במתקנים שכאלה נושאים, לרוב, אופי דומה לזה של משחק ארגוני, וליתר דיוק – של תחרות בין צוותים. דוגמה ידועה לכך היא התרגיל הבין-לאומי Locked Shields של נאט"ו, הנערך אחת לשנה במרכז המצויינות שלו בסייבר (CCD COE) שבטאלין, אסטוניה.

⁴⁶ ניתן אומנם לפתח יכולת פנים-ארגונית בתחום הזה, אולם, בראייה של העלויות הכרוכות בפיתוח, בשימוש השוטף ובאחזקה ארוכת-הטווח, אל מול אלה הכרוכות במיקור-חוץ, ניכר שמאמץ זה כדאי ומשתלם רק עבור ארגונים גדולים במיוחד (וקן, שלא במפתיע, ארגונים מדינתיים כדוגמת גופים ביטחוניים שונים).

ניהול התרגיל

כדי לממש כהלכה את שליטתה במהלכו של תרגיל תפעולי ברמה האופרטיבית והאסטרטגית, על המנהלת בראש ובראשונה להקים לעצמה מרכז שליטה תרגילי (להלן, בקיצור - משל"ת), שבו ובאמצעותו ינוהל התרגיל הלכה-למעשה. במקביל, תציב המנהלת תצפיתנים במרחבי התרגול, שישמשו לה כעיניים וכאוזניים. בהמשך לנאמר בגוף המדריך בעניין מגבלותיו של מרכיב הסימולציה בתרגול המעשי, חשוב להדגיש כי מושא המעקב של התצפיתנים הוא בכל מקרה תפקוד אנושי (של בעלי תפקיד וצוותים) ולא תפקוד של מערכות ותשתיות, דהיינו - התבטאויות מילוליות של בעלי תפקיד בעבודתם השוטפת ובמסגרת פורומים שונים, וכל מידע זמין נוסף, המונגש על גבי צגים או באמצעות מסמכים כתובים.

התצפיתנים יעמדו בקשר שוטף והדוק עם המשל"ת, ודיווחיהם ישמשו את המנהלת לביצוע הערכת מצבו של התרגיל (להבדיל מהערכת מצבו של הארגון, שאותה מבצעים המתורגלים). פעולה זו יש לבצע כ"ברירת מחדל" לפחות פעמיים ביממה (קצת אחרי תחילת יום התרגול ולקראת סופו), ומעבר לכך, בכל עת שיסתמן כי הקצב והכיוון שבהם מתקדם התרגול אינם עולים בקנה אחד עם המתוכנן.

ככלל, נכון יהיה למקם את התצפיתן שהוקצה לעקוב אחר פעילותו של מרחב תרגול מסויים ב"מרכז העצבים" החולש על פעילותו של המרחב הזה (כך, למשל, בהקשר לדוגמה של תרגול קונצרן הייצור שהובאה בנספח א', נכון יהיה להציב את תצפיתן ההנהלה הראשית של הארגון באתר שבו מקיימת ההנהלה את הערכות המצב שלה. דין זהה חל על התצפיתנים שיוצבו במפעלים של הקונצרן. ייתכן גם שהמנהלת תציב תצפיתנים בעמדות פיקוח על תשתיות הייצור של המפעלים).

מחמת הפיזור הפיסי של המתורגלים, וגם לצורך תמיכה בשליטה במהלכי התרגיל, רצוי לבצע את העברת הידיעות התרגיליות באופן ממוחשב.⁴⁷ לאור האמור לעיל, ובהנחה (הסבירה למדי) שבארגון אין בנמצא תשתית תקשוב ייעודית לשם כך, הטוב ביותר יהיה להשתמש לשם כך במערכת המסרים שתשרת את התקשורת בין המתורגלים לבין עצמם במהלך התרגיל. יש רק לוודא, שהתשתית המדוברת מאפשרת העברה הן של מסרים כתובים והן של קבצי מולטימדיה (קבצי קול וסרטונים). מומלץ להגדיר במערכת שנבחרה חשבונות משתמש ייעודיים לתרגיל, שייצגו את כל הגורמים המתורגלים, וישמשו הן אותם עצמם לצורך תקשורת ביניהם במהלך התרגול, והן את המנהלת, כדי שתוכל להעביר אליהם את הידיעות התרגיליות.

המנהלת עשויה לבצע במהלך התרגיל פעולה המכונה "עצירה מתודית" של התרגול. מדובר, בעצם, בעצירת תהליך העברת הידיעות למתורגלים לפרק זמן מוגדר, וכתוצאה ישירה מכך - בהקפאה של תהליך ההתפתחות של התרחיש לפרק זמן זה. פעולה זו עשויה לשרת שתי מטרות: האחת - מתן שהות למתורגלים לבצע הערכת מצב משוחררת מאילוץ זמן, כמו-גם מן הצורך להתמודד עם אתגרים חדשים שהתרחיש מתוכנן לזמן להם; והאחרת - מתן אפשרות בידי המנהלת לדלג בעקבות זאת על שורת ידיעות

⁴⁷ השימוש באמצעי תקשורת ממוכנים יאפשר לתעד באופן אמין, נוח ונגיש את המידע ש"זרם" במהלך התרגיל בין המנהלת למתורגלים ובין המתורגלים לבין עצמם, וכך, בסיס המידע שיווצר כתוצאה מכך ישמש כמקור מידע ראשון במעלה לתחקור התרגיל.



תרגיליות שטרם הועברו למתורגלים, הן כיוון שהובן על ידה שמטרת משנה תרגילית מסויימת, שהן נועדו להשיגה, כבר הושגה, או על מנת לקדם באופן יזום ומלאכותי את התגלגלות התרחיש התרגילי, לאחר שזה התקדם בקצב איטי יותר מהמתוכנן.

הכנה טכנית ולוגיסטית של סביבת התרגול

בגוף המדריך הובאה כבר התייחסות לעניין זה, שנגעה בהיבטים הטכניים והלוגיסטיים המשותפים לתרגול העיוני והמעשי. כמו-כן, בראשיתו של נספח זה הובאה התייחסות לעניין הזה בהקשר של תרגיל תפעולי ברמה הטכנו-טקטית. להלן, אפוא, מובאים היבטים המיוחדים לתרגיל תפעולי ברמה האופרטיבית והאסטרטגית:

- כמו במקרה של התרגול העיוני, כך גם בתרגול המעשי המאמץ הטכני והלוגיסטי העיקרי של המנהלת מתרכז בהקמה ובהיערכות של אתר אחד - הלא הוא המשל"ת. בשונה מן התרגול העיוני, בתרגול המעשי על המתורגלים להשקיע מאמצי היערכות משלהם, וזאת, לצורך הקמת סביבת התרגול שלהם. מודגש, שאחריות זו מוטלת על המתורגלים, ולא על המנהלת.
- קביעת מיקומו של המשל"ת, ותכנון ארגונו התפקודי והיערכותו הפיסית נעשים במסגרת תהליך ההיערכות הכולל של המנהלת לקראת התרגיל, ועליהם להסתיים במועד שיאפשר להביא את המשל"ת ליכולת תפקודית מלאה לא יאוחר מיומיים לפני מועד תחילת התרגיל.
- כמו בתרגיל שולחני ובמשחק ארגוני, כך גם בתרגיל תפעולי יש לקיים הליך של רישום המשתתפים עם פתיחת התרגיל (הדבר נכון לכלל מרחבי התרגול, לרבות המשל"ת), ולהמשיך בבקרת הנכנסים אל מרחבי התרגול עד למועד סיומו של התרגיל. גם כאן, יש לצייד כל משתתף בתג זיהוי אישי.
- בשונה מהתרגול העיוני, בתרגול המעשי אין כמעט משמעות לביצוע הפסקות של התרגול ביוזמת המנהלת, שכן, כל אחד מן המתורגלים מתפקד במסגרת הזו באופן דומה, ככל האפשר, לאופן שבו הוא פועל במצב האמת.