

# פיקוד ושליטה בצבא

## סקירה כללית\*

קירק קירכהופר

### פגיעות

כתוצאה מההישענות הגוברת והולכת של מפקדים בכל הרמות על מערכות לפיקוד ולשליטה, הן נעשו מטרות ראשונות במעלה לפעולות אויב. מערכות מתוחכמות לפיקוד ולשליטה נעשו יותר רכוש גונות; וכתוצאה ממורכבותן, הן הרבה יותר פגיעות. לפיכך, קיום פיקוד-ושליטה יעילים תוך שלילת יכולת הפיקוד-והשליטה של האויב הפך לשיקול טקטי ראשון במעלה. לדבר זה חשיבות מיוחדת בעיקר בימים הראשונים של מלחמה קונבנציונלית, כשיכולת הפיקוד והשליטה של כל צד תהיה גורם מכריע בקביעת התוצאה הסופית.

לשרידותה ולפעולתה הרצופה של מערכת צבאית לפיקוד ולשליטה קיימים שלושה גורמים בעלי חשיבות מיוחדת: ● מיגון פסי: על התכנון להביא בחשבון את הסביבה הקשה שבה פועלת המערכת וכן את האפשרויות לנזק פסי,

תוכנו ונכנו. עתה מתברר, שהכרחי לתת למערכות לפיקוד ולשליטה קדימות דומה למערכות הנשק שבהן נועדו לתמוך.

### התפיסה

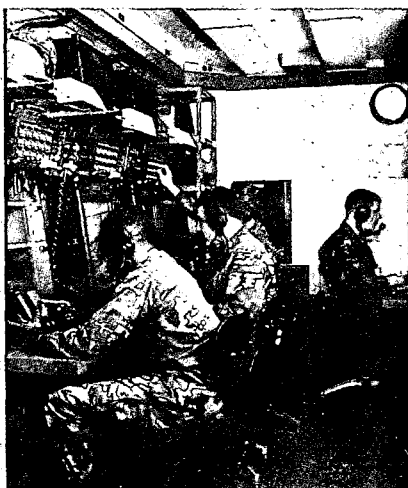
מערכת לפיקוד ולשליטה חייבת לספק לכל המפקדות, בכל הרמות, נתונים עדכניים, בטוחים ומדויקים, שיאפשרו למפקד לתכנן, להנחות, לתאם ולשלוט בכוחות הכפופים להן במהלך משימה מסוימת. המערכת נועדה לעקוב אחרי המצב בשטח נתון, וברזמנית לאסוף, לעבד, להעריך ולהפיץ מידע על האיום. בסיסית, נועדה מערכת לפיקוד ולשליטה לסייע למפקד צבאי לפרוס את כוחותיו במקום הנכון, בזמן הנכון, ובהיקף הדרוש, גם כשהוא נתון להתקפה.

באופן כוללני ניתן להגדיר מערכת לפיקוד ולשליטה כמערכת משולבת, הכוללת מספר רכיבים הנוגעים לדוקטרינה, לנהלים, לארגון, לכוח האדם, לצידוד, למתקנים, לקשר ולדיווח. נראה שההיבט החשוב ביותר הוא שילוב המערכות לפיקוד ולשליטה\*\*\* במערכות הנשק. כך, כאשר מתכננים מערכת הגנה יש לכלול בה משלב מוקדם מאד בתהליך התכנון לא רק כלי נשק, אלא גם רכיבים עיקריים לפיקוד ולשליטה — חישנים, ציוד קשר, מרכזי פיקוד, מחשבים, צגים ומסופים, לרבות ציוד כיטחון קשר.

\*\*\* בשנות השבעים דנו במערכות לפיקוד ולשליטה ולמידע (CCIS). מאוחר יותר התקבלה ההשקפה שקשר מאובטח מהווה חלק חיוני מהמרכבת, והשתרש המונח C<sup>3</sup> — פיקוד, שליטה וקשר. מאוחר יותר התוספו תחומי פעילות נוספים: C — נוסף מסמל מחשבים (Computers); CM — אמצעי-נגד (Counter-measures); I — מודיעין (Intelligence).

יש קרבות שגורלם נחרץ לשבט או לחסד, בגלל תקשורת טובה או גרועה. לפני מלחמת ה' עולם השנייה ובמהלכה רשת התקשורת הותאמה בפשטות למבנה הארגוני, מרמת פיקוד אחת אל רעותה. שיטה ישירה זו התאפשרה עקב התנועה הייטית יחסית של כוחות היבשה. לעומת זאת, גרמה השיטה לריכוז מידע במפקד דות השונות. מידע ומודיעין עין הועברו כלפי מעלה, והחלטות ופקודות הועברו כלפי מטה, אל המפקדה המבצעת ואל מרכזים שונים בעורף. בדרך כלל, נעשה שימוש בצורה גולמית כל שהיא של העברת נתונים, או באלחוט דיבור ובטלפרינט-רים. הצפנת האלחוט הייתה עדיין בחיתוליה.

המונח פיקוד ושליטה (C<sup>2</sup>)\*\* השתרש בשנות הששים, כשהופיעו המערכות הראשונות לפיקוד ולשליטה, שנועדו לפעול בסביבה שבה רמת האיום בלתי מתוחכמת, יחסית. רמת האיום גדלה מאז בצורה ניכרת, אולם המערכות לפיקוד ולשליטה לא הדביקו, בדרך כלל, את קצב ההתפתחויות. יותר מעשרים שנה לאחר שהופיעו בראשונה, נחשבות מערכות לפיקוד ולשליטה כציוד משני, שניתן לצרפו למערכות נשק מאוחר יותר, וזו הייתה הגישה לציוד הצפנה. ברוב המקרים מוסיפים ציוד כזה לאחר שמערכות לפיקוד ולשליטה, או לתקשורת, כבר



חיל הנחתים האמריקני יכניס בקרוב לשימוש מערכת ניהול אש אוטומטית שתסייע למפקדים לנהל את הקרב ביעילות.

\* המאמר תורגם מ-International Defense Review, ינואר 1983.  
\*\* C<sup>2</sup> — Command & Control.

אנוש, ומערכת אוטומטית באה תחתיו. לאמיתו של דבר, כמעט כל המערכות לפיקוד ולשליטה כבר מבוססות על מחשבים זעירים, מהירים ומקוונים לעיבוד נתונים.

כאשר מציגים בפני המשתמש מערכת חדשה לפיקוד ולשליטה, נתקלים בבעיות תפקודיות ומבצעיות רבות. אחת החמורות בהן היא הסתייגותו של המשתמש. יש להביא בחשבון שמפקד מורגל כשיטות הידניות המקובלות עליו מזה זמן רב. אפילו כשמגדירים את הרעיון של מערכת חדשה לפיקוד ולשליטה מרגיש המפקד (כמי שאמור להשתמש במערכת), שאין היא נוחה לשימוש, למרות שיישומה של מערכת כזו ייעשה במתכונת קונבנציונלית. ייתכן שיקשה עליו להבין מה טיבה האמיתי של המערכת ומה השלכותיה על תפקוד ומבצעים.

למערכות לפיקוד ולשליטה רכיביהן הבסיסיים דומים מבלי להתייחס לסביבת פריסתן:

★ חישני סריקה ואיכון מטרת אוספים מודיעין על פעילותם של כוחות האויב, תנועותיהם ומיקומם.

★ עורקי תקשורת בין החישנים למרכזי הפיקוד ולכוחות.

★ מרכזי פיקוד. כל הנתונים על כוחות האויב והכוחות הידידותיים מעובדים במרכזים אלה ומוצגים בפני המפקדים כדי לאפשר להם להעריך את האיום ולהורות על תגובה מתאימה.

★ תת-מערכות לניווט (בעלות חשיבות מיוחדת לצוללות נושאות טילים בליסטיים).

מערכות לפיקוד ולשליטה חייבות לכלול את ארבעת הרכיבים הבסיסיים הנזכרים. בנוסף, המערכות חייבות להיות משולבות עם המערכות הסגורות השונות המצויות בשדה הקרב (כגון לוחמה אלקטרונית, הגנה נ"מ וסיוע התקפי קרוב).

המטרה היא לשלב מודיעין, תקשורת ועיבוד נתונים אוטומטי (עני"א) כמערכת אחת, שחשבו בעבר כמערכות עצמאיות (כגון מערכות ארטילריית השדה), כדי שיהפכו ליישום חדשה — מערכת לפיקוד ולשליטה. הגדרת מערכות לפיקוד ולשליטה ותכנון חייבים להיעשות בקפדנות אם הכוונה שיביאו לחיזוקי המידע הדרושים בשדה הקרב המודרני. היעד העיקרי לתכנון חייב להיות סיוע למפקד "לנהל את הקרב", ולקבל החלטות קשות — החלטות הכרוכות ביותר משתנים מכפי שהמוח האנושי מסוגל להתמודד עמם. בדרך כלל, פתור



לפיקוד ולשליטה להתמודד, נוסף לכך, עם תופעות מגוונות, ובכללן פעימות אלקטרו-מגנטיות. השימוש בטכניקות מוליכים-למחצה (בציוד אלחוט ועיבוד נתונים) ובכבילים (לטלפונים ולעורקי טלפרינטר טקטיים) מעמיד בספק את שרירות הציוד לפיקוד ולשליטה במלחמה גרעינית.

הכוחות המזוינים טרודים בקיום מערכת יעילה לפיקוד ולשליטה לנוכח מאמצי האויב לשבשה ובשיפור אמצעייה ללוחמה אלקטרונית, כדי לפגוע ביעילות במערכת האויב לפיקוד ולשליטה. יש צורך לזהות את עורקי התקשורת החיוניים ביותר של האויב. אלה עשויים להיות פגיעים לתקיפה בנשק וכאמצעי נגד. לכך יש להחזיק בתוך המערכת לפיקוד ולשליטה פירוט של הסדר"כ האלקטרוני של האויב.

עורקי התקשורת בתוך המערכות לפיקוד ולשליטה הופכים ליעדים חשובים לניצול ולתקיפה אלקטרונית. בעורקים האלה עובר מידע על מצב כוחות האויב וכוחות ידידותיים, והם מספקים את האמצעים להעברת פקודות והנחיות. לפיכך, הצפנה מהווה מרכיב חיוני במערכת לפיקוד ולשליטה.

## תכנון מערכת לפיקוד ולשליטה

כדי להשיג רמה גבוהה יותר של יעילות קרבית ולעשות שימוש טוב יותר במשאבים הזמינים, יש צורך לקבל החלטות בעיתן. יש צורך במחשבים מהירים יותר, כדי שידרש פחות זמן לאיסוף המידע ולעיבודו. הצורך לקבל החלטות מייד נעשה כה חיוני עד שבמקרים מסוימים יצאו הדברים, למעשה, מכלל שליטה

חבלה או שרכיבים יפלו בידי האויב. חיוני ביותר, שאפשר יהיה לנתב מחדש את רשת הקשר, במהירות ובקלות, אם חלקים ממנה נפגעו בשל פעילות אויב, או שיש להעתיקם בשל תנועת כוחות.

● יציבות הקשר והתעבורה: שינויים סביבתיים עלולים להשפיע על הזרמת הנתונים בין הצמתים השונים ולחייב שינוי ניתוב של הודעות והקצאה מחודשת של עורקי תקשורת. המוקדים צריכים להיות מתוכננים איפוא באופן שיהיו מסוגלים להתמודד עם העומס הגובר כתוצאה מכך.

● לוחמה אלקטרונית: (ל"א) אפשר להשתמש בלוחמה אלקטרונית כדי לפגוע באיכות הערוצים שבשימוש; כדי לשבש כליל את השימוש בהם (על ידי חסימות); וגם כדי לזרוע מבוכה (על ידי החדרת מידע כוזב לתעבורת הקשר). חיוני איפוא לשלב ציוד לביטחון קשר במערכת לפיקוד ולשליטה כבר משלב התכנון המוקדם.

לוחמה אלקטרונית היא האיום העיקרי על מערכות לפיקוד ולשליטה (להוציא מתקנים נייחים באחרים מוקשים). אמצעי נגד אלקטרוניים עלולים לשבש בצורה פעילה את פעילות רשת הפיקוד והשליטה, בעוד שאמצעים אלקטרוניים עלולים לנצל את יכולת רשת הפיקוד והשליטה בצורה סבילה. ברגע שנתגלה, אפשר לזהות את האיום של אמצעי הנגד האלקטרוני ולאכנו בזמן כמעט-אמיתי. כך ניתן לקבוע איוה סוג של ציוד מופעל, וכלפי אילו יחידות ומערכות הוא מכונן. בעוד שבמלחמה קונבנציונלית ניתן לצפות לאמצעי נגד אלקטרוניים בהיקף ניכר, בסכסוך גרעיני יהיה על מערכת



חות בפני המפקד יותר אפשרויות מכדי שיהיה מסוגל להעריך בעצמו. יש לסייע לו, ולא להממו בצגים ובתדפיסים. יש להגן עליו מפני מידע שאינו שייך לעניין, ולהציג בפניו רק מה שהוא חייב לדעת. כתוצאה מכך, יש צורך להשיב על מספר שאלות בסיסיות בשלבים המוקדמים של תכנון מערכת לפיקוד ולשליטה:

(א) האם תיתכן מערכת העונה על הדרישות הצבאיות?

(ב) האם מסגרתה של המערכת נכונה?

(ג) מה תהיה ההשפעה של המערכת

החדשה על הארגון הקיים?

(ד) האם התכנון הטכני נכון?

בדומה לכך, יש להשיב תוך כדי שלב התכנון על סדרה של שאלות הנוגעות לביצועיה של המערכת המתוכננת:

(א) איזה שטח צריכה המערכת

לכסות?

(ב) כיצד תפעל המערכת בשילוב עם

מערכות אחרות?

(ג) האם המערכת צריכה להיות ניידת?

(ד) מה צריכה להיות יעילות ניתוב

השדרים של מערכות התקשורת?

(ה) מה צריכה להיות עמידותה של

המערכת לחסימות, להונאה, לגילוי

ולאיכון?

## ציוד

את הציוד המצוי במערכת לפיקוד ולשליטה ניתן לחלק לשלושה סוגים: מרכז הפיקוד, חישנים וציוד תקשורת.

מרכז הפיקוד מורכב מציוד לתקשורת פנים בתוך המרכז ומערכות מידע ידניות ואוטומטיות. המערכות האוטומטיות כוללות מעבדים מרכזיים, מאגרי תוכנה ויחידות תצוגה, לרבות מנגנונים משולבים ומתקנים הדרושים לניהול המערכת בדרך כלל.

המשתמש ירצה שלציוד שלו יהיו טווח חים ויכולת מספיקים לשימוש בכל מצב. צריכה להיות מהירות פעולה גבוהה, המאפשרת לקבל החלטות מייד, בתנאים סותרים. המערכת צריכה להיות מאובטחת, כדי לוודא שלאויב לא תהיה גישה לשום מידע. ולבסוף, הציוד צריך להיות אמין, ומסוגל לפעול בסביבה של אמצעי נגד אלקטרוניים.

רמת האלקטרוניקה בימינו מאפשרת כמעט כל מהירות, עצמה ויכולת נדרשים, בציוד קטן וקל, ברמת אמינות שלא נודעה כמותה לפני עידן המעגלים המודפסים והשילוב בקנה מידה נרחב.

כבר עתה ניתן לחזות ציוד יעיל לפיקוד ולשליטה, עדיין קיימים כמה גורמים מגבילים, כגון רמת ההגנה שאפשר להק-

המכ"מ שנועדה לספק את הסימנים הראשונים להתקפה. הסריקה נעשית ברמות פיקוד רבות, וכוללת כיסוי מתחת לפני המים, על פני השטח ובאוויר — כשמטחי הנשיאה נעים מאוניות ומטוסים ועד לוויינים. כל החישנים חייבים להיות משולבים במערכת מקיפה לפיקוד ולשליטה, שבאמצעותה הם מסוגלים לספק למרכזי המודיעין והפיקוד מידע בזמן אמיתי.

ברמה האסטרטגית נועדו החישנים להתמודד עם האיום מצד הטילים הבליסטיים. כדי לצמצם הזעקות-שווא משתמשים — ככל האפשר — לפחות בשני סוגים של חישני התראה. את הטילים עצמם, למשל, ניתן לזהות במכ"מ, בעוד שחישן תת-אדום המותקן בלוויין עשוי לגלות את השיגור. חישנים תת-אדומים משמשים לגילוי פיצוצים גרעיניים. ידוע, שארצות הברית עוסקת בפיתוח רשת חדשה של גלאי פיצוצים גרעיניים, המורכבים בלוויינים.

ברמה הטקטית אפשר להשתמש במכ"מים, בחישנים תת-אדומים, בתצפיות אופטיות, במדי-טווח לייזר ובציוד סיוע אלקטרוני כדי לאסוף נתונים על האויב.

## תקשורת

תקשורת היא המרכיב החיוני ביותר במערכת פיקוד ושליטה. בלעדיה אין ערך למידע שנאסף על ידי החישנים ולנתונים שעובדו במחשבים. במערכות מודרניות לפיקוד ולשליטה שמים דגש אפוא על אמינות עורקי התקשורת, הציוד והנהלים ובטחונם.

תקשורת מהירה, אמינה ובטוחה מאפשרת למפקד לכוון את פעילות כוחו

נות נגד חסימות. חלק מהליקויים במערכת לפיקוד ולשליטה נובעים מצורת הנייח, בעוד שליקויים אחרים נובעים מהקצב המהיר של ההתפתחות הטכנולוגית. ליקויים אחרים מתרחשים באקראי עקב חוסר תשומת-לב לאפשרויות הקיימות בטכנולוגיה, או אפילו עקב הערכה בלתי נכונה של מגבלותיה.

במקרים רבים מתוכננים חישנים בודדים להיפרס לבדם, ולמערכת הסריקה בכללותה יש כושר נותר או שרידות מעטים בלבד. יתר על כן, במקרים רבים אין הכיסוי בחישנים קרקעיים נגד מטוסים מנמיכי-טוס. תחום בעייתי אחר הוא תחום הפעילות המשולבת. יש צורך, למשל, לשפר את שטחי הפעילות המשותפים בין מערכות קרקעיות להגנה נ"מ לבין מערכות קרקעיות וימיות אחרות. ייתכן שאחד הליקויים החמורים ביותר הוא היעדר יכולת חסינה מפני הפרעות לזיהוי מהיר לטווחים ארוכים. הרכיבים הקרקעיים של מערכת זיהוי כוזריכים להיות משולבים לחלוטין במערכת כות עתידיות לפיקוד ולשליטה.

מערכות לפיקוד ולשליטה לצרכי הגנה והתקפה פועלות כיום, בדרך כלל, בנפרד, למרות שרבות משימותיהן זהות. הארגונים העצמאיים הקיימים כיום, למשל, לצרכי פעילות אווירית הגנתית והתקפית אינם יעילים כדי לשלוט במטוסים רב-תכליתיים. מתכנני המערכות העתידיות חייבים לשקול בכובד ראש את שיפור תזרים המידע בין הארגונים הללו ובתוכם.

## חישנים

החישנים החשובים ביותר, הקשורים במערכת לפיקוד ולשליטה, היא רשת



תיו ולתאמה עם מפקדים אחרים. ברמה האסטרטגית נדרשים אמצעי קשר אמינים ושרידים ביותר לטווחים ארוכים, אם כי בעלי קיבולת נמוכה, יחסית. בדרך כלל מנצלים את כל קשת התדרים מתחום ה-VLF (עד 30 קילוהרץ) עד ה-SHF (3 עד 30 גיגאהרץ) כדי להשיג את הגמישות הדרושה לפיקוד ולשליטה על צוללות אסטרטגיות, מפציצים וטילים בליסטיים הפרוסים ביבשה. לתקשורת טקטית משתמשים בדרך כלל בתדרים גבוהים לטווחים בינוניים ועורקי ת"ג (HF) ו-תג"מ (VHF) לטווחים קצרים. אפשר להשתמש בטכניקות הצפנה, דילוג ספרתי בין תדרים וספקטרום מורחב לצרכי ביטחון וחסינות לחסימות. עם גבור הצפיפות בתעבורת הקשר הצבאי נעשה ניהול התדרים חיוני.

קשה ויקר יותר לאבטח את עורקי התקשורת הקולית. בעבר פיגרה אבטחת התקשורת הקולית אחרי הצפנת השדרים והנתונים. עתה מאפשרות טכניקות חדשות התייעצויות אישיות החיוניות במערכת לפיקוד ולשליטה.

מערכות לפיקוד ולשליטה חייבות לטפל בתעבורת נתונים רבה יותר מאשר תעבורה קולית. בנוסף רבות מתת המערכות המבוססות על מחשבים ומהמהירות המבצעיות מחוללות אותות ספרתיים (דיגיטליים). רמת המחשוב גדלה, בעיקר כדי לנפות את כמויות הנתונים האדירות הללו ולאפשר למפקד לשלוט בסביבה רוויית מידע.

בעיות שילוב מתעוררות לעתים קרובות, כאשר מקשרים בין שתי מערכות מחשבים באמצעות רשתות תקשורת. בדרך כלל מתגברים על כך על ידי מה שמכונה "רשתות נתונים": משתמשים בתוכנה (כלומר, שינוי צורת השדר) כדי להתגבר על בעיות החומרה. אמצעים לתקשורת נתונים חייבים להיות, למרות זאת, בעלי אפיונים תקינים של שידור וקליטה.

בשל ריבוי הצידוד האנלוגי המצוי עדיין בשימוש, חייבות תת-מערכות התקשורת במערכת לפיקוד ולשליטה להיות מסוגלות לטפל הן באותות אנלוגיים והן באותות ספרתיים. אולם מגמת המעבר לצידוד ספרתי פירושה, שהמערכות העתידיות יטפלו רק בתעבורה ספרתית. גם התקשורת הקולית תהפוך לספרתית.

בשעת התקפה יש להתייחס אל התקשורת במערכת כאל מטרה ראשונה במעלה, מפני שרשת זו תשמש להנחות את הכוחות ששרדו להתקפות נגד. לכן, הרשתות הקלאסיות, המשתמשות בעור-

קים יחידים וישירים, אינן שמישות עוד. הנטייה היא איפוא לכיוון של מה שמכונה "מערכות אזוריות", שבהן מקימים מספר צמתי תקשורת, המהווים רשת לתקשורת עם יחידות המפוזרות על פני שטחים נרחבים, ומה שחשוב מכך – מאפשרת ניתוב חלופי של שדרים במקרה של השמדת חלק מהרשת. עתיד גדול נשקף לרשתות, שבסיסן קרקעי ומפעילות עורקי תקשורת נל"נ ומעין-נל"נ (כגון נתיבי השתכרות קרניים), שישלבו חסינות לחסימות וניידות, הדרושים בסביבה של שדה הקרב העתיד.

את הדרישות לתקשורת במערכת לפיקוד ולשליטה ניתן לתמצת כך:

(1) תצורת רשת התקשורת חייבת להיות שת-וערב, כדי לאפשר התמודדות עם השמדה חלקית. כל צומת חייב להיות

נייד; זמני פריסתו והתקפלותו קצרים; (2) כל צורות ההתקשורת, ובכלל זה התקשורת קולית, באמצעות טלפרינטר, פכסימיליה, נתונים ונתונים גולמיים – חייבות להיות זמינות;

(3) חובה שתהיה אפשרות של שיחות ועידה ושידורים;

(4) עורקי התקשורת חייבים להיות מאובטחים;

(5) המערכת חייבת להיות מסוגלת לטפל בתעבורה אנלוגית וספרתית כאחת, כאשר ההמרה מאנלוגית לספרתית מבוצעת אוטומטית בתוך המערכת;

(6) המערכת חייבת להיות חסינה לנשק גרעיני;

(7) קטע המערכת, העוסק בשידור

ובקליטה, חייב להיות בעל יכולת אוטומטית להמרת מהירות השידורים; (8) יש צורך לספק אמצעים לניהול תדרים.

בשנים האחרונות היו לתקשורת בתדרים גבוהים ובאמצעות לוויינים כאחד השלכות ניכרות על התקשורת במערכות לפיקוד ולשליטה, בייחוד ברמה האסטרטגית. פיתוחה של התקשורת באמצעות לוויינים בארצות הברית האפיל בתחילה על תקשורת בתדרים גבוהים מפני היתרונות הניכרים של הראשונה, בייחוד בכל הנוגע לקיבולת התעבורה. כשהתברר בשנים האחרונות שהלוויינים עלולים להיות פגיעים וכי עורקי תקשורת באמצעות לוויינים עלולים להיות משובשים בעיתות משבר, התגלה בארה"ב עניין מחודש בתדרים הגבוהים. עתה מתבצע שם מאמץ ניכר כדי לשפר את הצידוד לתדרים גבוהים, המוזנח מזה זמן רב. שאר העולם ממשיך להישען על התדרים הגבוהים לצורך קשר בטווחים ארוכים. בנוסף נשקף עתיד לשני אמצעים חדשים יחסית: לייזרים וסיבים אופטיים. שניהם יספרו ניכרות את תחום התדרים הרחב בטווחים הקצרים לצרכי שידור מידע, וינוצלו להפצה מקומית של תעבורת מודיעין רחוקה ולחילופי נתונים בין מערכות נפרדות בשדה הקרב.

יש להתייחס להשימוש בסיבים אופטיים במערכות לפיקוד ולשליטה יגבר במידה ניכרת. קיימות לכך סיבות רבות. כבילים של סיבים אופטיים מאפשרים ביטחון משופר מפני שהם עמידים, יחסית, בפני חבלה. הכבילים קטנים, קלים וזולים; יוצרים השראה וקרינה זניחות (העדר הקרינה מקטין את האיום מצד טילים המתביתים על קרינה); השפעות ברקים ופעילות אלקטרומגנטיות על כבילים של סיבים אופטיים קטנות מאד. בנוסף, הם בעלי קיבולת גדולה להעברת נתונים (עד 45 מגאביט לשנייה) ובעלי גורם הקלשה נמוך של האות (4dB לק"מ). ניתן לקיים עורק של סיבים אופטיים עד 8 ק"מ ללא מגברים.

כמו בתחומים אחרים, הייתה למיקרו-פרוססור השפעה ניכרת גם כאן. רכיב אוניוורסלי זה הכפיל את יכולת החישוב בפריטים רבים פי עשרה, ואפילו פי מאה. ההשלכות של המיקרו-פרוססור באו לביטוי לא רק בצידוד, כגון מרכזיות שדרים, אלא גם במתקני מחשבים היקפיים. הייתה לו השפעה ניכרת על איפיון מבצעי של צידוד קשר. רבים מהתפקידים שהיה צריך לבצע במרוכז במעבדים בינוניים ניתנים עתה לביצוע בטכניקות של ביזור העיבוד.

גם לטכניקות של תשדורת ספרתית משופרת הייתה השפעה ניכרת על התקשורת במערכות לפיקוד ולשליטה. אף על פי שאין הטכניקות חדשות, אין ספק שיש לראות התקדמות טכנית חשובה ביכולת להמיר מייד תקשורת קולית (אנלוגית) לצורה ספרתית, ולהיפך. יתרון רב משמעות הטבוע בטכניקה הספרתית הוא קלות הטיפול במידע בצורה בינארית תוך כדי תהליכי הצפנה ופענוח בצידוד הצפנה, ופישוט האבטחה של התקשורת. התקדמות רבה נעשתה בתחום הצידוד הרב-ערוקי. מכשירי הצפנה רב-ערוקים נמצאים עתה בשימוש, כשם שמצויים מכשירים לשידור ולקליטה בעלי ששה, שמונה, שנים עשר ויותר ערוקים. ברמת הקורפוס והזירה נפוצים מכשירים בעלי 24, 48 ו-96 ערוקים.

רוב הדברים שתוארו עד כה ייתכנו מבחינה טכנית וטכנולוגית, אך לרוע המזל, אנו רחוקים עדיין מיישומם. הצידוד המצוי בזרועות הצבא השונות סובל מליקויים שונים. ייתכן שהגדול בליקויים הוא פעילות הגומלין בין הזרועות השור נות, או אפילו בין ענפים שונים בתוך אותה זרוע הנוכעים, למשל, מחוסר התאמה של נהלים, תקנות, אופני שידור או מהירויות שידור. רוב צידוד התקשורת אינו מסוגל לפעול בקצב הגבוה של שידור רים ספרתיים הדרוש לקשר בין רשתות של חישנים, מרכזי פיקוד ויחידות טקטיות. לעורקים הקיימים חסרה קיבולת מספקת כדי לאפשר חילופי מידע בזמן אמיתי בין אנשים, בין מחשבים או בין אנשים למחשבים. יתר על כן, מכשירי קצה איטיים, כגון מכשיר לקליטת שדרים על גבי סרט מנוקב, גורמים לעתים קרובות לעיכובים ניכרים.

בין הליקויים החשובים נמנים – פגיעות לאמצעי-נגד אלקטרוניים, לפעילות אלקטרומגנטיות ולתקיפה פיסית, ניידות מוגבלת וזמני פריסה והתקפלות ממושכים באופן בלתי סביר. קיימים גם ליקויים מיוחדים, כגון היעדר יכולת לשיחות ועידה אוויר-אוויר והיעדר אפשרויות התקשורת מעבר לקו הראייה; שניהם עשויים להיות חשובים לטייסים. למרות שרוב העורקים מעבירים מידע רגיש חסרים ברובם אמצעי הצפנה. לעתים קרובות, אין די צידוד לביטחון הקשר, או שהצידוד אינו זמין בכמויות הדרושות.

## פעולות נגד

מטרת הפעולות נגד מערכת לפיקוד ולשליטה היא להקטין בצורה משמעותית את

יעילות כוחותיו של האויב בהתקפות מתואמות על האלקטרוניקה הקשורה בחישנים, בתקשורת, בצידוד הניווט ובמרכזי הפיקוד של האויב.

פעולות נגד מערכת לפיקוד ולשליטה אינן מצטמצמות בשום פנים לתקיפה פיסית ולהשמדה. גישה אפשרית אחרת, המנצלת את תלותו של האויב במערכות אלקטרוניות טרם הקרב, למשל, היא להציג בפני האויב תמונה כוזבת, אך אמנה. פעילות נגד המערכת לפיקוד ולשליטה יכולה להיות יעילה רק אם פרטי התקשורת, האמצעים המשולבים והנהלים המצויים במערכות של האויב ידועים, ומאפשרים לזהות מרכיבים מסוימים כמטרות.

## הטיפול במידע וההגנה עליו

אחת מאמות המידה העיקריות שיש לשקול כאשר מתכננים מערכת לפיקוד ולשליטה היא אומדן כמות המידע שתטפל בו. יהיה זה גורלי אם המידע יוגבל רק למידע על האויב. אולם מודיעין כזה, מצד שני, מלא תמיד תפקיד חיוני בפיקוד ובשליטה, ולעתים קרובות סיפק את חולית המידע העיקרית הדרושה כדי להטות את הקרב. יתר על כן, אין תחליף לידיעה בזמן אמיתי של הפעילויות והאירועים.

טמונה סכנה בהצפת המפקד בנתונים זמינים רבים. יש צורך איפוא להעביר אליו אך ורק את הנתונים הדרושים לו, ועליו לקבלם בזמן הנכון ובמקום הנכון. יתר על כן, יש להפיץ את המידע רק לאלה המורשים לקבלו. עם זאת, בסיס הנתונים חייב להישמר בשלמותו, ולהתעדכן עם המידע המתקבל.

ליקוי חשוב במערכות קיימות הוא הכמות הגדולה והבלתי נחוצה של הפצת נתונים וחילופיהם. במערכות העצמאיות של קהיליית הביטחון יהיו נתונים (כגון מידע על חנאי מזג האוויר המקומיים), שאין צורך להפיצם; כך ייחסך זמן יקר. אין ספק שקיימות טכניקות כדי לפקח על פעילות גומלין כזו.

דרישות בסיסיות הן ביטחון הקשר וחסיונות לחסימות. התקשורת הצבאית מצויה כיום בתקופת מעבר בין תעבורה שכמעט כולה גלויה לעידן שבו תהיה כמעט כל התעבורה מוצפנת. כאשר זה יושלם, לא יהיו מסוגלים לירות את כל התעבורה, לפענחה ולשאוב ממנה את נתוני המודיעין בתחומי זמנים שבהם אפשר עדיין להפיק תועלת מן המידע. התוצאה ההגיונית מכך תהיה חסימות מוגברות, כדי למנוע שידורים כלל.

אין אפשרות להגן על כל השידורים. אחד הפתרונות יהיה להגן רק על שידורים נבחרים נגד יירוט וחסומים. אולם אין זה קל לקבוע אילו שידורים יחוסנו, מפני שגם התעבורה שאיננה מוגנת חשוכה למישהו. האם יכולים לוותר על הגנה על נתוני ירי של ארטילריה, או שנתוני ההצבה והתחמושת לא יגיעו ממרכז ניהול האש אל התותחים? מצד שני, האם הצפנת כל השידורים, עד לסוללות התותחים (או אפילו לתותחים עצמם) לא תסבך ותסחוט ללא צורך את מערכות הקשר ואת זרימת התעבורה?

על המשתמש מוטל איפוא להגדיר בשיתוף עם מתכנן המערכת מה העורקים שעליהם יש להגן. לגבי כל עורק יש צורך לקבוע אם דרוש ביטחון קשר או ביטחון השידורים. בביטחון הקשר מצפינים את הנתונים המשודרים, בעוד שבביטחון השידורים ייתכן שהנתונים גלויים אבל השידור כולו מוגן. ביטחון השידורים מתוכנן כך שהתקשורת כולה תהיה מוגנת מפני האזנה וניצול על ידי הסתרתה, למשל, בין רעשים אקראיים-כביכול.

עם הופעת המיקרו-פרוססור, צמח דור חדש של ציוד לביטחון קשר, והופיעו טכניקות חדשות. הטכנולוגיה החדשה ביותר מאפשרת להשתמש בצורות חישוב מורכבות שונות, ועורקי התקשורת נעשים על ידי כך הרבה יותר בטוחים. לא זו בלבד שהמיקרו-פרוססור איפשר לתכנן ציוד אוטומטי להצפנה, מהיר ובעל יכולת גבוהה, המספק רמה גבוהה של ביטחון, אלא שהוא גם איפשר לייצר ציוד קטן יותר, קל יותר וזול יחסית. כתוצאה מכך, ניתן עתה לחזות שימוש נרחב באמצעים לביטחון קשר בעתיד הקרוב. התפשטות זו תצריך ניהול מתאים של מפתחות ההצפנה.

תחום חדש, העוסק באבטחת מערכות קשר הוא תחום ביטחון המחשבים. הובעה דאגה ביחס למחשבים, מפני שהם מעבדים מידע מסווג ובלתי מסווג ברמות שונות בתוך אותו מכשיר. כיום משתמשים בתוכנה ובחומרה כאחד כדי לוודא ביטחון בכל הרמות.

במערכות קיימות לפיקוד ולשליטה מצויים כל כך הרבה מחשבים ומיקרו-פרוססורים מכל הגדלים, המבצעים מגוון כה רחב של משימות, עד שקל מאד להעלים עין מביטחון המחשבים. קיימת גם מידה מרובה של הפצת נתונים מיותרת. התפיסה הזו בקשר להפצת המידע מהווה מקור לדאגה לרבים ממתכנני המערכות ולמשתמשים בהן. כאשר שותפים למחשב משתמשים מקומיים ומרוחקים

כאחד, לא זו בלבד שהם שותפים למידע ולעיבודו, אלא שהמערכת עצמה משתרעת על פני רמות שונות של ביטחון. יתר על כן, קווי שידור, מרכזיות ובקורות מסופים עשויים להיות נחלתם של מספר משתמשים במקומות שונים, והם עשויים להתגלות לאנשים ברמות שונות של ביטחון. מובן מאליו, שקיימות אפשרויות בכוח להפרות ביטחון. יש הכרח למדוד את הגישה לנתונים מסווגים. יתר על כן, יש למנוע ממתכנני המערכות והיישומים מליצור תקלות, שמאחר יותר אפשר יהיה לנצל תוך תוצאות הרסניות.

## חסימות

הדעות חלוקות בשאלה אם להאזין למערך-כות קשר (ולנצלן בצורה סבילה), או לחסום אותן. במשך שנים התנגדה קהילת מודיעין הקשר למאמצים לפתח מערכות נגד חסימה, בנימוק שהאויב יכול להשיג על ידי האזנה יותר מאשר על ידי חסימה. אולם בהתחשב ברמת הביטחון המושגת כיום על-ידי ציוד ההצפנה עלול היריב להעריך את סיכוייו לפענח את החומר כנמוכים ביותר; ולפיכך, הוא עלול להחליט לחסום מערכת לפיקוד ולשליטה, כדי לשבשה. האפיון הראשוני של מערכת לקשר טקטי הוא איפוא שרי-דוט, חסינות לחסימות, תוך סבירות נמוכה של האזנה.

מכשירי חסימה מופיעים בכל הצורות, הגדלים והתצורות. יש יבילי-אוויר המכ-וונים נגד משדרים המוצבים על הקרקע; יש מתכלים, המוטלים מן האוויר בתוך שטח האויב; או שהם ממוקמים על הקרקע, מקושרים ביניהם ומכוונים נגד לוויינים. לוויינים המשמשים כמגברים הם מטרות מעניינות, בשל התעבורה הרבה העוברת דרכם. כפי שכבר הוזכר, עשויה החסימה להציף את אותות הקשר, ולהוציא את הלוויין מכלל שימוש. מנקודת ראות גיאוגרפית, קל למדי לחסום לוויין, מפני שהוא נראה משטח גדול.

קיימות טכניקות לחמיקה מחסימות. על פי אחת התפיסות — "הכוונת אפס", הישימה למערך אנטנות מסודר לפי תחומים — מעובדים האותות הנקלטים על ידי האנטנה בצורה דינמית, והקלטת בתחומים השונים מותאם כדי לקלוט בצורה מוגברת בכיוון האות. שיטות אחרות מבוססות על טכניקות של שידור אותות. השיטה שמרבים ביותר לדבר בה בימינו היא דילוג בין תדרים: המכשיר משדר בתדרים רבים עד 200 פעם בשניה. הדילוג חייב להיות מהיר דיו כדי לחמוק מן החסימות, ויחד עם זאת לא מהיר מדי, כך

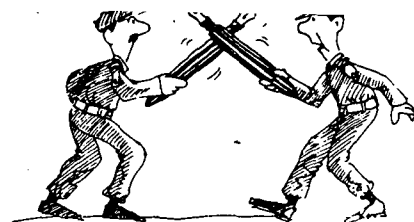
שמחיר הציוד יהיה גבוה מדי. שיטה אחרת משתמשת בקוד בסדרה ישירה — שיטה המצריכה מכשיר קידוד להעתקת תדרים — או שילוב של קידוד בסדרה ישירה ודילוג בין תדרים. גישה רביעית, דילוג עתי, קשה מבחינה טכנית ומצריכה תכנית שינויים, הפועלת במהירות גבוהה.

## הדדיות

הדדיות בין מערכות לפיקוד ולשליטה כוללת את התאמת המערכות זו לזו, התאמת המערכות בין הזרועות השונות, התאמה בין מערכות הקשר הקשורות בכך (טקטיות ואסטרטגיות כאחת) והתאמה בין כוחות של מדינות ידידותיות. אחד מתחומי ההדדיות שאין מרבית להזכירו הוא השיתוף בין מערכות ביטחוניות (ובייחוד מערכות לפיקוד ולשליטה) לבין גופים שאינם צבאיים, כגון שלטונות הדואר, המשטרה וגופים העוסקים בתובלה.

מובן מאליו שתקינה היא הדרך להשיג הדדיות. המשמעות היא לא רק תקינה של נהלי הפעולה וחומרה משותפת, אלא גם תקנים בנוגע לצורת השדרים, הן במערך-כות המבוססות על אותיות וספרות, והן במערכות המבוססות על ספרות בינאריות ("ביטים"). היבטים אלה של מערכות לפיקוד ולשליטה מהווים בסיס לחילופי מידע, ולפיכך גם בסיס להדדיות. רמת המחשוב של מערכות לפיקוד ולשליטה תוכל להשתפר רק אם יגבר שיתוף הפעולה בתוך המערכות ובניהן.

אם לא יינקטו בעוד מועד צעדים כדי לפתור את הבעיות ההדדיות, ייתכן שהזיוג בין מערכות לפיקוד ולשליטה של הרמות הגבוהות לבין אלה של הדרגים הנמוכים יותר ועם מערכות הנשק עצמן ייעשה קשה ביותר. כדי להעריך נכונה את בעיות ההדדיות, אפילו בתוך מערכת לפיקוד ולשליטה, יש צורך להתבונן במערכת כרשת רבת-זרועות. בקורפוס שבו מספר דיוויזיות ייתכנו 200 או יותר מִרְכָּזֵי עיבוד, מבלי לכלול את צמתי הקשר. ציוד לשידור נתונים מסוגים שונים מקיים את הקשר בתוך הרשתות הללו, החל בעורקי מיקרו-גל ו"טרופו" ועד מעגלי חיוג להעברת קול, רשתות אלוט קרבות ומערכות בעלות כניסות רבות תוך פיצול זמן. בחינת הרשתות האלה מגלה שהצרכים, ושיקולי ההדדיות של כל קהילייה שונים עד כדי כך שאין זה מעשי לצפות שכל הקהיליות יאמצו להן שיטה אחידה, תקנית ומסוג אחד.



כות מהווה ערכות מדינית לקביעותנו במקום, יחד עם אותה מידת הכוונות הנחרטת על-ידי הגנה מרחבית, אם בונים כזאת. מה שאומר ש' לרר לגבי הגלעד וכו' — ודאי שהגבולות הטבעיים של ארץ ישראל (המדבר והים) טובים יותר מכל גבול אחר, אך בכך איננו עוסקים כאן. אין אנו מציעים "לכבוש" מולדת כיבוש יזום, כפי שנעשה על-ידי יהושע בן-נון. בפועל נתבעת עתה מאתנו הבחירה בין חזרה לגבולות 1948 לבין שמירת גבול הירדן. גבול הירדן מאפשר עיכוב פריצת-פתע עד לגיוס המילואים, בשעה שגבול 1948 אינו מאפשר זאת.

גם ההערה בדבר ההיסטוריה מסלפת את הצגת דברי לא הבאתי כלל עובדות לגבי דרכים לכבוש את ארץ ישראל. דנתי בשאלה של אחיזה בארץ ישראל. אומות שישבו רק על החוף נעקרו מהר. מי שהיכה שורשים בשלד ההררי של הארץ, החזיק בה תקופה ארוכה בהרבה. איזכור כיבוש הארץ על-ידי יהושע מופיע במאמרי כאנלוג לתסריט הבסיסי שהצגתי, כמעט לתפארת המליצה. כתבתי: "מה שנמשך שנים רבות בימי יהושע, יכול להימשך ימים אחדים בלבד כשהמדובר בשריון מודרני" — מה כאן אינו תואם את המציאות? כל הדרגמאות המובאות על-ידי ש' לרר אינן משנות עובדה זאת במאומה, הן רק מסיחות את דעת הקורא מעצם העניין. המלה "דמגוג" גיה" המובאת על-ידי ש' לרר תואמת יפה תרגיל זה.

כאמור, אין לאמיתו של דבר מחלוקת גם עם ה"יונים" בישראל לגבי ערכו של השומרון, וספרו של א' שלו יוכיח. המחלוקת היא אחרת: האם זהו מצב זמני, ואכן קרובים הימים שבהם אפשר יהיה להתעלם משיקולים ביטחוניים — או שמא יימשך מצב זה עוד עשרות שנים לפחות, ועל-כן צריך לעבור לפתרונות של ישיבת קבע (ואני מתעלם כאן משיקולי זיקתנו לכל חלקי ארץ ישראל). ועוד הערה: ברוחב הפוליטי הישראלי מודגש ההבדל בין ליכוד למערך, בין שמירה על כל איזור יהודה ושומרון לבין שמירה על בקעת-הירדן וגוש עציון (כשאת גב ההר מוסרים לשלטון ירדן בתנאי פירוז). אך מושינגטון או מקהיר או מרבית-עמון נראים הדברים אחרת. במבט משם אין כל הבדל בין ההתנחלות באלון מורה לבין זו שבמעלה אפרים. כאשר ניהל עמנו המלך חוסיין משאומתן באמצעות קיסניג'ר בשלהי 1974, פתח בדרישה לנסיגת כוחותינו דווקא מכל בקעת-הירדן!

החתך הפוליטי המשמעותי, על כן, איננו בין אותם שני מצעים לפתרון, שבשדה ניהם מצרפים למדינת ישראל שטחים "כבושים". בעיני ירדן, מצרים ואותם ערבים המוכנים לדבריהם לקבל קיום ישראל, יש אכן שוני בין מי שסומך על "שלום" וחוזר לגבול 1948 — לבין מי שאינו סומך על הסדר פורמאלי. כל זה, כמובן, מעבר לעמדת אש"ף — שאינה מוכנה לקבל אף את מדינת 1948. אשר לי — הבאתי במאמר רשימת

ההסכמים והפירושים שלא נתקיימו, ולדעתי די גם בהם על-מנת שלא נסכן את קיומנו על סמך הסדרים כאלה. אפשר "לנסות" בגזרות אחרות, וסיני היה ניסיון גדול — אך לא במקום שבו כישלון יכול להתבטא בהיעלמותנו מן המפה. מבט על המזרח-התיכון בחמש השנים האחרונות יוכיח, שאף בין הערבים לבין עצמם אי אפשר לסמוך על שלום פורמאלי. האיזור מלא תהפוכות לבקרים, ללא קשר עם הסכסוך הערבי-ישראלי: אפגניסטן עם תחילת הפיכה ולאחר מכן מלחמה מתמשכת; אירן עם הפיכה נגד השאה, הפיכה נוספת נגד הנשיא הראשון (המסתתר בפריס), ורצח הנשיא השני; עירק עם תקיפת אירן ברגע שנראתה לה חלשה; סוריה והריגת 3,000 איש בחמת אשתקד; שמונה שנות המלחמה בלבנון; שתי הפיכות נפל בסעודיה; שני נשיאים שרצחה דרום-תימן בצפון-תימן ואחד שנרצח בדרום-תימן על-ידי צפון-תימן; רצח סאדאת; כיבוש צ'אד על-ידי לוב, נסיגתה וכיבוש מחודש של המחוז הצפוני שלה; פלישה שלא נתקיימה (עקב התערבות הצי השישי) של לוב בסודן בראשית השנה; מלחמת הפוליסריו נגד מרוקו בסיוע אלג'יריה — אין, כמדומני, ספק שאזורנו אינו מזכיר את שלוות סקנדינביה של ימינו, והראגה הביטחונית מחייבת.



## המשך מעמ' 19

המדינה.

נראה ששלושה הם התחומים העיקריים לבעיות: תפיסות הניהול והשליטה, תחום הנתונים המשולבים (ובו צורת השדרים, נהלים וכיוצא באלה), שיתוף פעולה טכני (נהלי שידור, טכניקות של תיאום וכד'). בתחום האחרון, למשל, יהיו פריטים כגון מחברים ולוחות משולבים כרוכים בצד החומרה. כדי לאפשר לשתי רשתות לפעול תוך הדדיות יש צורך בתיבה משולבת, או במה שמכונה "כניסה", המבצעת תפקידים כגון הכוונה, חציצה, המרת קצב העברת הנתונים וני-

תוב. כך מסוגלות אפילו שתי מערכות בעלות מבנים שונים של חומרה ותוכנה לפעול במשולב.

מערכות לביטחון, כגון מכשירי הצפנת נתונים, ציוד להצפנת קול ומסופים להצפנת מסמכים, מציבים בפני ההדדיות קשיים מיוחדים. אפילו בתוך אותה זרוע של הכוחות המזוינים קיימות רמות שונות של דרישות לביטחון, המצריכות ציוד מסוגים שונים, כאשר הדרישות המיוחדות של קהילות משתמשות בקשר שונות מניבות מיגוון רחב של ציוד קשר קווי ואלחוטי וציוד לביטחון קשר.

קשה עוד יותר היא ההדדיות בין מערכות של זרועות שונות, או בין כוחות ממדינות שונות. לרוע המזל, אפילו הזרועות השונות במדינה אחת פיתחו נהלים להחלפת מידע באופן עצמאי. לפיכך, למרות שבתיאוריה אפשר להחליף כמות ניכרת של מידע בין מערכות אוטומטיות ולעבדן, מונע היעדר ההדדיות שימוש מוגבר במערכות אוטומטיות לפיקוד ולשליטה מעבר לתחומי הזרוע או