**אסטרטגיה וחידושי סייבר – 2/4/2019**

מהפכות בעניינים צבאיים - סייבר:

האקדמיה טוענת שמה שקורה היום בתחום הסייבר דומה מאוד למה שעברה האקדמיה בשנות ה-20-30 של המאה ה-20 וכן בשנות ה-40-50 של המאה ה-20, זאת משום שבדרך כלל מהפכות בעניינים צבאיים נגזרות מטכנולוגיות מסוימות. השינוי הטכנולוגי מחייב בחינה מחודשת של אופן בניית וארגון הכוח.

בשנות ה-20 וה-30 – מדובר על הופעת הטנק והמטוס בתקופה שלאחר מלחמת העולם הראשונה, כשהשאלה היא האם המלחמה הבאה תיראה כמו מלחמת העולם הראשונה; ובשנות ה-40-50 – הכניסה לעולם הטילאות והגרעין, כשאסטרטגים שואלים את עצמם האם האופן בו נבנו הארגונים הצבאיים מתאימים לתקופה הנוכחית.

הטענה היא כאמור שהיום אנחנו נמצאים בתקופה די דומה, ונשאלת השאלה האם סייבר – המהפכה הקיברנטית – הוא רק המשכה של מהפכת הופעת המעבד או שמדובר בדבר חדש. בהמשך לכך יש חמש שאלות ששואל היום כל מי שעוסק בעיצוב שדה הקרב העתידי, והחיפוש אחר תשובות מתקיים אצל מדינות רבות – רוסיה, סין, איראן, ועוד. התשובות של כל אחת מהמדינות לשאלות האלה די שונות – בהתאם לתרבות של כל אחת מהן.

השאלה הראשונה: האם אכן מדובר במהפכה בעניינים צבאיים? האם הסייבר משנה באופן משמעותי את ניהול המלחמה?

השאלה השנייה: האם עידן קיברנטי וסייבר מעצים את הצד התוקף או את הצד המגן.

השאלה השלישית: מהי מהות ההרתעה והכפייה בעידן הקיברנטי והאם הן בכלל קיימות? האם יש דבר כזה כמו התראה מוקדמת בעולם קיברנטי?

השאלה הרביעית: האם סייבר מעצים את השחקנים החזקים או את השחקנים החלשים יותר?

השאלה החמישית: האם סייבר ונוכחות כלים קיברנטיים בארגז הכלים תורמים ליציבות אסטרטגית או דווקא מערערים אותם.

**שאלה ראשונה: האם הסייבר אכן מהווה מהפכה בעניינים צבאיים?**

צה"ל מתלבט כבר מספר שנים בשאלה האם יש מקום לפתוח אגף סייבר. בכל מדינה יש תשובה אחרת לשאלה האם יש מקום או לא לפתוח זרוע קיברנטית. שאלות נוספות: כמה כסף להשקיע ועל חשבון מה. אם יוחלט שזו מהפכה בעניינים צבאיים – ההשקעה וההצטיידות צריכים להיות בהתאם.

יש שתי אסכולות מתחרות: אסכולה אחת טוענת שזו מהפכה שמגמדת כל דבר אחר שהכרנו קודם, וזה המוד העיקרי של שדה הקרב העתידי. הטענה היא שכלי קיברנטי הוא בדיוק כמו הופעה של נשק גרעיני – כלי שהוא בפני עצמו, לא כתוספת לכלים אחרים שיש לנו בארגז הכלים הצבאיים יודע להכריע את המלחמה – דהיינו לכפות את הרצון האסטרטגי שלנו על הצד השני (כהגדרת קלאוזביץ). כלים קיברנטיים יודעים לעשות התקפות מדויקות, תפורות בדיוק לאפקט שאנחנו רוצים ליצור, על חשבון מימדי לחימה במרחבים אחרים, בים באוויר וביבשה ומרחיבים באופן משמעותי את רפרטואר התקיפות שאפשר לעשות בלי לצאת מהבית – מה שגם מקטין את החיכוך הבין לאומי האפשרי. זה גם מאפשר למדינות שבדרך כלל לא מאפשרות להקרין עוצמה, כן לשדר עוצמה ולמרחקים שהם דיס פרופורציונליים לעוצמה הכלכלית שלהם. הטענה היא שסייבר פותח דומיין חמישי של המלחמה, בנוסף לים, יבשה, אוויר וחלל.

יצוין כי גם ביחס לסייבר אין הגדרה קנונית, אך מקובל להבדיל בין חתרנות קיברנטית – מאמצים שיודעים לשבש את המערכת היריבה, לבין תקיפות שבקצה שלהם יודעים גם לייצר אפקטים קינטיים – למשל כלי שמפסיק לעבוד או משהו שיכול להתפוצץ, עד כדי למצב של הכנסת עיר שלמה לחושך או יצירת פיצוץ גרעיני קטן.

האסכולה השנייה מתנגדת לכך, וטוענת כי אין פה שום דבר חדש. מזמן כבר אנחנו מדברים על מלחמה מבוססת רשת ועל אפקטים, והסייבר הוא רק שיפור וחדשנות של מה שכבר הכרנו קודם לכן. עוד טוענים באסכולה זו שסייבר כשלעצמו לא מסוגל לייצר ניצחון בשדה הקרב ולהביא לכפיית רצוננו על היריב. זה יכול להיות כלי תומך משמעותי, אך במלחמות הגדולות, הכלי הזה מחוץ לארבעת הדומיינים הקלאסיים לא יכול לעשות שום דבר, והוא אמור להיות מעטפת לכל הכלים האחרים.

שאלה מעניינת היא – מתי סופרים את המהלומה הקיברנטית הראשונה. יש טענה שכבר בשנות ה-80 היה פיצוץ בצינור גז בסיביר שפגע בכלכלה הסובייטית, אשר נבע ממאמצי סייבר. אם כך, טענת המתנגדים, היא כי יש כבר קרוב לארבעה עשורים של פעולות קיברנטיות, אולם לא הייתה מלחמה קיברנטית של ממש שהוכרעה באופן כזה.

בין 2006 ל-2016 הוקמו פיקודי סייבר רבים בעולם, כלומר עיקר האנרגיה הייתה ביחס לאסכולה הראשונה; ובשנים האחרונות יש נטייה קצת יותר לאסכולה השנייה. אך כאמור במדינות שונות רואים את הדברים אחרת, ועדיין האסכולה שמצדדת ברעיון של RMA קיברנטי ובכך שמדובר במהפכה, היא האסכולה השלטת.

**שאלה שנייה: האם הסייבר מעצים את הצד התוקף או המגן.**

גם ביחס לשאלה זו יש שתי אסכולות, וההשלכה היא משמעותית. הפונקציה ההגנתית וההתקפית בישראל לא יושבות תחת אותו פיקוד וההכרעה בשאלה זו יכולה להשליך על השאלה מי יקבל יותר משאבים.

אלה המצדדים בכך שהסייבר מעצים את הצד התוקף טוענים שמבחינה מעשית – אף פעם אי אפשר לייצר הגנה הרמטית, ולכן עדיף לקיים מחקר טוב איפה יש פתח שבו אפשר להתגנב ולתקוף – מכאן שהצד התוקף חזק יותר.

כמו כן הצד התוקף יגרום בדרך כלל לצד השני להגיב. מי שחווה מהלומה קיברנטית בונה לה מגננה. לצד התוקף מספיק להצליח רק פעם אחת, לעומת הצד המגן שצריך להצליח פעם אחר פעם.

כמו כן לא צריך להיות מעצמה כדי לייצר כלים התקפיים. לעומת זאת כן צריך כלים מאוד קשים לפיתוח על מנת לייצר כלי הגנה. מעבר לכך ההגנה תמיד תהיה מחולקת – שכן הצד התוקף יכול להחליט אם הוא תוקף את החלק הפרטי או הציבורי (הסקטור הפרטי לא תמיד מקבל על עצמו את הרגולציות שמוציאות רשויות הסייבר ומחייבות את הסקטור הציבורי – זה רלוונטי בעיקר לסקטור העסקי שלא רוצה שיגבילו אותו בכל מיני דרכים). כל אחד שמשתמש במחשב מעדיף לחשוב על נוחותו מאשר על משמעת וביטחון – ולפיכך הצד התוקף תמיד יוכל לחדור פנימה.

האסכולה השנייה טוענת מנגד שפיתוח כלי התקפי אמיתי שיודע ליצור אפקטים קינטיים במדינה זה מאוד יקר (כאשר מדובר בכלי למשל שיודע לחדור פנימה ולשנות דרך פעולה של צנטריפוגות). לפיכך רק מעצמה יכולה להרשות לעצמה את זה. התקפות קרימינליות פשוטות יותר הן יותר קלות לביצוע, אך חדירה למערכות פיקוד ושליטה אסטרטגיים זה משהו ששמור למעצמות. כך שתקיפה אולי טובה לריגול ולשיבוש החיים, אך פיתוח כלי התקפי משמעותי יותר מתאים לשחקנים מאוד מצומצמים.

עוד טוענת אסכולה זו שהגנה היא יותר אפקטיבית בסייבר, שכן אפשר לבנות שכבות שונות של הגנה, ולשנות אותן כל הזמן. גם הצד המגן יכול לבנות מלכודות ותחבולות ולגרום לצד התוקף לחשוף את זהותו.

גם ביחס לכך אין תשובה ברורה וגם בצה"ל מתקיימים וויכוחים על נושא זה.

**שאלה שלישית: האם ההרתעה קיימת בסייבר?**

כזכור יש שני סוגים של הרתעה. אם רוצים למסד הרתעה יציבה האיום שלנו צריך להיות אמין. האמינות מורכבת מיכולת ומנחישות. אנחנו מראש לא יכולים להפגין את היכולות בעולם הקיברנטי. היכולת היא פעמים רבות, חד פעמית. שימור היכולת ואי חשיפתה מביאים לכך שבפועל אי אפשר ליצור הרתעה.

במקרים רבים אנחנו מעדיפים את המרחב הקיברנטי כי יודעים לייצר אפקטים בלי שהצד המותקף יודע לשייך זאת למדינה התוקפת. הרוסים למשל יודעים לעשות זאת כל הזמן.

כמו כן פעמים רבות הצד שתוקף אותך קיברנטית לא מספיק דיגיטלי כדי שתוכל לתקוף אותו בחזרה. למשל – ארה"ב או ישראל הם שחקנים רציניים בשדה הקיברנטי, אבל עלולות להיות מותקפות על ידי שחקן שלא עוסק מספיק בנושא סייבר.

המשמעות היא שגם לא ניתן לייצר הרתעה מסוג שלילה- אי אפשר להציג שיודעים מספיק טוב להתגונן מפני התקפה, אלא רק להתגונן מפניה בהצלחה.

עוד שאלה היא – מה הם סימנים ראשוניים להתקפה קיברנטית? שהרי הרתעה פעמים רבות היא בתגובה לסימנים ראשונים לכוונה לתקיפה. זה משנה את כל נושא המודיעין.

לכן הטענה היא שאף אם התראה מוקדמת אפשרית בסייבר היא מאוד בעייתית.

מנגד יש טענה שהרתעה היא בהחלט אפשרית גם בעולם הקיברנטי, שכן יכולות הזיהוי הקיברנטי משתפרות כל הזמן והיום יותר קל מאשר פעם לזהות תקיפה קיברנטית. טענה נוספת היא שבשנים האחרונות חל שכלול משמעותי בנושא יכולות הגנה, ספיגה והתמודדות עם התקפה קיברנטית. בהמשך לכך נטען שבתחום הזה צריך להיות כל הזמן בחיכוך עם הצד השני, ומדי פעם לעשות "דקירות" קיברנטיות שאולי אמנם חושפות מעט את היכולות שלנו, אבל מרתיעות ומשדרות לשחקן השני את המסר המתאים.

מעבר לכך יש סימטריה הפוכה – אפשר להרתיע מפני תקיפה קיברנטית לאו דווקא באיום קיברנטי בתגובה. למשל מזכיר המדינה האמריקאי הזהיר שאם תהיה תקיפה קיברנטית על מתקני גרעין אמריקאיים, תישקל תגובה קינטית כנגד התוקפים.

**שאלה רביעית – האם הסייבר מחזק שחקנים חזקים או חלשים.**

גם כאן יש שתי דעות. אם מדובר בכלי שיודע לשנות סדרי עולם – אז רק מדינות ומעצמות יכולות לבנות כלים כאלה. רק מדינה יכולה לבנות כלי שיכול לנתק מתקשורת או לשתק כוחות מזויינים של מדינה אחרת. היכולת הקינטית היא מכפיל כוח בכל שאר מימדי העוצמה שלו. אם אכן מדובר במהפכה – צריך להיות שחקן חדש בכל המימדים. נכון שאפשר לבצע הטרדות קטנות ברמה הקיברנטית, אבל אם באמת רוצים לעשות משהו רציני צריך להיות מעצמה.

הגישה הפוכה טוענת שזה כלי שיודע לתת לשחקנים קטנים מאוד, אפילו לא מדינתיים, יכולות גבוהות מאוד. למשל – יכולת פריצה לטלפון היא לא יכולת מורכבת או מסובכת מדי, וגם שחקן לא מדינתי יכול לעשות משהו די דומה.

**שאלה חמישית**  - **מה הסייבר גורם לעולם – האם הוא יציב יותר או פגיע יותר**

דעה אחת – הסייבר הופך את העולם להרבה יותר פגיע ולוחמני. פעם כדי להילחם במדינה היית צריך לפלוש אליה. לעומת זאת בעולם הסייבר אין כללי משחק. אפשר לעשות הרבה דברים בלי להשיג תגובה מהצד השני. בנאטו יש שאלה למשל – האם תקיפה קיברנטית של אחת המדינות (למשל המדינות הבלטיות) גורמות להפעלת סעיף 50 וליציאה להגנה אליה? זו לא שאלה תיאורטית, כי הרוסים יודעים לפעול במישור זה ולהסב נזק רב למדינות אלה. עניין זה מעלה את מספר האינטראקציות האסטרטגיותבאופן שיוצר גם השלכות הלאה.

דעה שנייה – כל מה שתואר לא מהווה מלחמה, כי אנשים לא מתים במאסות והיציבות האסטרטגית די נשמרת. מאחר ועולמנו הופך להיות יותר ויותר מחובר דיגיטלית זה מייצר סוג של ריסון עצמי. למשל – הרוסים מסוגלים להפיל היום את הבורסות בכל העולם; אך הכספים של רוב האוליגרכים הרוסים מוחזקים בבורסות האלה. לפיכך זה הופך את העולם ליותר בטוח.

מנגד אפשר לטעון שהעולם הפך לסופר מסוכן – מספר שחקנים קטנים יכולים לייצר אפקטים יותר גדולים ממה שידענו אי פעם, וזה גם מעודד מירוצי חימוש בין מדינות. אין היום בעולם רגולציה בין לאומית או אמנה בין לאומית בתחום הקיברנטי. מדינות שונות גם מגדירות באופן שונה מהו סייבר, וזה נותן פתח לאותם מירוצי חימוש.

מאחר שגם אין הסכמה מהי צורת תפקוד חזקה יותר – הגנה או התקפה – אך מרבית האנשים בארגונים צבאיים נוטים יותר לכלים התקפיים, יש נטייה חזקה בכל העולם לפתח כלים התקפיים. אחת הדרכים להפעיל כלי התקפי בעולם קיברנטי היא לחדור למערכת היריבה. כלומר הרבה שחקנים מעודדים את הארגון שלהם להיות בחיכוך קיברנטי עם האויב. בסייבר גם אין עומק אסטרטגי. הזמן שלוקח מתחילת התקפה ועד להגעת קצה ההתקפה למרכז הכובד יכול להיות שניות. אם זה כך, הרי שבאופן מאוד משמעותי זה מצמצם את זמן התגובה. מכאן שיש יותר ויותר נטייה לפתח יכולות "יום הדין" קיברנטיות, ולהפוך מערכות פיקוד ושליטה לכמעט אוטומטיות – שברגע שמערכת תעבור תקיפה, היא תדע לעבור לתגובה אוטומטית מבלי שיהיה אדם באמצע. אנחנו יודעים שאוטומטיזציה של מערכות גרעיניות כמעט והביאה את העולם לאסון גרעיני – ומכאן אפשר להקיש גם על ההשלכות אוטומטיזציה מערכות פיקוד ושליטה אחרות.

בחינת הגישה הרוסית לסייבר – אמנות המערכה הרוסית בתחום הקיברנטי

הרוסים לא מייחסים למונח סייבר כמונו. סייבר מכונה אצל הרוסים "מאבק המידע" – מפני שבמקור החשיבה שלהם על לחימה קיברנטית מגיע משלושה מקורות:

מקור ההשראה הראשון הוא מקור דיגיטלי – טכנולוגי - ה-IT RMA – הרעיון שלפיו הניצחון לא יגיע מהשמדה שיטתית של מערך האויב, אלא מיכולת לפגוע במערכות פיקוד ושליטה שמחזיק האויב, ולגרום להן להפסיק לתפקד. הם הבינו שהם פחות דיגיטליים מהאויב ושהאויב מאוד נשען על מערכות דיגיטליות, עניין שגם הפך להיות מקור פגיעות עבורו, ולכן פיתחו כבר בשנות ה-80 כלים של לוחמה אלקטרונית לפגוע בכך.

מקור השראה שני – מהתחום המודיעיני. משנות ה-20 יש במודיעין הסובייטי מסורת של "active measures" – פעולות מודיעיניות מניפולטיביות, במטרה לעצב דעת קהל של חברות ומנהיגים במקומות שונים – במסגרת כל נושא ייצוא המהפכה. במערב מכירים את זה יותר כלוחמה פסיכולוגית או לוחמת מודיעין. ברוסיה הסובייטית זו היתה דיסציפלינה מאוד מפותחת בעולם המודיעין. הם האמינו שבאמצעות כלים רכים כאלה אפשר להשיג אפקטים מאוד משמעותיים, וטוענים שהפסידו במלחמה הקרה בגלל שהאמריקאים הפעילו נגדם לוחמת תודעה שיצרה מבפנים חתרנות משמעותית ופירקה את המדינה. הנושא הזה הוא מוטיב מאוד משמעותי מבחינה אסטרטגית – ופחות מצוי במערב כשמדברים על סייבר.

מקור שלישי – המילה סייבר. ברוסיה היתה דיסציפלינה כבר בשנות ה-60-70 במסגרת האקדמיה, במדעי הטבע והלימודים מדויקים שעסקה בלימודי קיברנטיקה. זו היתה דיסציפלינה מדעית שעסקה בתהליכי קבלת החלטות במערכות מורכבות. מערכת מורכבת יכולה להיות כל דבר – החל מגוף האדם וכלה במפעלים גדולים או כלכלה של מדינה. זה גם שייך לתחום המחשוב. הרעיון היה – לנסות להשפיע על תהליכי קבלת החלטות של הצד השני.

כלומר – על פי הגישה הרוסית סייבר הוא סוג של לחימה שמטרתה להשפיע גם באמצעים דיגיטליים טכנולוגיים וגם באמצעים קוגניטיביים – פסיכולוגיים על תהליך קבלת ההחלטות של הצד השני.

לכן מרכז הכובד של מאבק המידע הוא תפיסת מציאות של חייל בודד, מטה כללי, חברה מסוימת או מקבלי החלטות – והרעיון בסייבר הוא לעשות מניפולציה על קבלת ההחלטות על מנת לייצר בראש של הצד השני תמונת מצב מסוימת ולגרום לצד השני להתנהל לאור תמונת המציאות הזו – שיכולה כמובן גם להיות כוזבת לחלוטין. כלומר שליטה רפלקסיבית – מנתבים את הצד השני באמצעים רכים.

הגישה השונה מביאה בין השאר לכך שקשה להגיע לרגולציה עם המערב לגבי השאלה איך מסדירים את הנושא. הרוסים מדברים על שדה קרב שמתנהל בשלושה מקומות: 1. כל המרחבים שבהם זורם המידע. בעוד שבמערב ברור שזה במחשב – ברוסיה המרחב הוא הרבה יותר רחב. גם מחשב, וגם רדיו, טלויזיה, שיחות עם בני אדם, רשתות חברתיות, וכל דבר שבו זורם מידע ויכול להשפיע על תפיסת המציאות שלך.

2. תוכן המידע – מה מופיע באותה טלוויזיה, אינטרנט, רשתות מחשוב וכו'.

3. תשתית טכנולוגית שנותנת ביטוי לשני המרחבים הראשונים.

כלומר כשמנהלים את מאבק המידע מבחינת הרוסים – מתנהלים בכל שלושת המרחבים. המשמעות היא שאין לרוסים צורך לסנכרן בין אנשים שיושבים בארגונים שונים – אנשי פסיכולוגיה, מודיעין ולוחמת מחשוב. אצלם זה מחובר אינטגרלית ואותו הגוף מפעיל את זה. אקט מאוד הוליסטי ומורכב – כי מנסים להשפיע על הצד השני גם באמצעים דיגיטליים וגם באמצעות תוכן, לתמרן את השחקן השני.

המשמעות היא שדברים כמו פגיעה קיברנטית מתקדמת, לחימה אלקטרונית, לחימה פסיכולוגית, הונאה – מה שאצלנו ובמערב יושב בארגונים שונים – אצל הרוסים אדם אחד שאחראי על מאבק המידע עושה את זה. אמנם גם אצל הרוסים יש גופים שונים שמטפלים בדברים ויש ביניהם מאבק יוקרה, אך כל מבצע של מאבק מידע יהיה מאבק משולב שמשלב בין כלל ההיבטים שבהם מדובר. זה גם יכול להתרחש בכל אחד מהמרחבים שיש בהם תחרות אסטרטגית – מרחב צבאי, דיפלומטי ועוד. מאבק המידע נועד גם להפעיל כלים אופטימליים להפעלת כוח קינטי.

הייחודיות בפעולה הסובייטית: איחוד המאמצים והניסיון לבצע סינרגיה בעולמות תוכן שונים. הפעולות בתחום המידע צריכים להיות מסונכרנים עם מהלכים קינטיים בשדה הקרב ועם מאמצים דיפלומטיים. דוגמה למשל – באסטוניה כשניסו לחולל מהומות סביב נושא פסל החייל הרוסי, הם ניסו לפעול גם און ליין וגם במקביל לפעול אוף ליין לצורך הפלת מוסדות שלטון באסטוניה. יש ניסיון להשפיע על מאסות במדינה, גם מבחינה תוכנית וגם מבחינה דיגיטלית – מפילים להם אתרים אלקטרוניים ממשלתיים, וכל זה לא מלווה בכוח קינטי.

בגרוזיה ב-2008 רואים דבר דומה למה שקרה באסטוניה – ניסיון לתקוע טריז בין האוכלוסיה להנהגה באמצעים קיברנטיים, במקביל להפעלת כוח קינטי חזק. כך גם באוקראינה ב-2014. הרוסים כבשו את חצי האי קרים והשתלטו על שטח שהוא יותר גדול ממדינת ישראל בפחות משבועיים, כשבשטח הזה ישנם 10,000 לוחמים חמושים אוקראינים. זאת למשל על ידי ניתוק מערכות פיקוד ושליטה, בלוקדות של מערכות אלקטרומגנטיות – בצד הקיברנטי – קינטי. נוצר מצב למשל, שבו הצי בקרים לא מסוגל לדבר עם הפיקוד בקייב עקב התקפות קיברנטיות. נותר מפקד של אוניית דגל של הצי האוקראיני – והרוסים עלו מולו ברשת והעלו ווטרן של המלחמה הפטריוטית הגדולה שנלחם בצי של הים השחור – כאשר שניהם מגיעים מאותו אזור תודעתי, והווטרן החל לשכנע אותו שכל מלחמה בין רוסיה לאוקראינה נדונה לכישלון, והם אחים, ויש לו יותר משותף עם הרוסים מאשר עם האוקראינים. בסופו של דבר אותו ווטרן שכנע את מפקד האוניה לא לתת פקודה להגן בצורה אקטיבית ולהסתער.

במקביל גורמים לאוכלוסיה המקומית להגיע לבסיסים של הצבא האוקראיני ולשכנע את החיילים להיכנע – והכל נעשה באופן משולב, בלי שהרוסים לוקחים אחריות על הכל, וטוענים שהאזרחים האוקראינים הם אלה שיזמו את המהלך לפנות לחיילים. עם זאת ידוע שבפועל הרוסים הפעילו אותם מאחורי הקלעים.

מעבר לכך אצל הרוסים אין הבדל בין פרטי לבין ציבורי. רוסיה יודעת גם לקחת אנשים עם רקע קרימינלי ועם מיומנויות גבוהה ולהעמיד אותם לרשותה. דוגמה – יחידות ווגנר שנמצאות עכשיו בסוריה, בחסות של כל מיני אוליגרכים, שבפועל מאומנות על ידי הצבא הרוסי ומקבלים ממנו מודיעין ועוד.

הרוסים עוסקים גם בהמשכיות ההשפעה. במערב חושבים על מבצעי סייבר כמעין "דקירה" או מבצע נקודתי. הם עוסקים במאבק המידע כאירוע בלתי פוסק, שאין לו התחלה, אמצע או סוף ברור. זה מתרחש במקביל ברמה הטקטית, האסטרטגית ועוד, וכחלק אינטגרלי מהתחרות האסטרטגית עם הצד השני. זה מאוד שונה מהדרך שבה אנחנו חושבים על זה במערב.

לחימה היברידית רוסית – מושג שבא לתאר את הגישה הרוסית העכשווית למלחמה. במערב כשמדברים על כך הכוונה היא לשילוב של צורות לחימה שונות, קונבנציונליות, תת קונבנציונליות, צבאיות ולא צבאיות.

ברוסיה – מתייחסים לכך כדוקטרינת גרסימוב – גנרל שמעודד את קציניו במטכ"ל הרוסי לחשוב על האופי המשתנה של המלחמה, שכן לדעתו אנחנו מצויים בעיצומה של מהפכה בעניינים צבאיים. להשקפתו במלחמה מודרנית יש שילוב של כלים צבאים וכלים לא צבאיים, ביחס של 4 ל-1 (לטובת מאמצים לא צבאיים). מאבק המידע הוא זה שמחבר בין המאמצים הצבאיים ללא צבאיים.

בשורה התחתונה: כשהרוסים חושבים על סייבר מדובר בדברים טכנולוגיים משולבים בדברים קוגניטיביים – פסיכולוגיים; מדובר באפקט לעיצוב תודעה של הצד השני; והמאמץ הוא הרבה יותר ממושך ורב מימדי מאשר במערב.

אין אצל הרוסים פיקוד סייבר, אלא תחרות בין מספר גופים, מי יקח אחריות על הנושא. המתחרים העיקריים הם אנשי ל"א, שכן יש במטכ"ל הרוסי אגף ל"א שכפוף ישירות לרמטכ"ל והוא מתחרה בעיקר מול אנשים מקהיליית המודיעין הצבאית והאזרחית ומול גופים שלכאורה אחראים מסורתית על לוחמה פסיכולוגית. יש אגף של פוליטרוקים שנפתח שוב ב-2018 אחרי שנסגר בשנת 1991 ועוסק גם הוא בנושאים האלה.