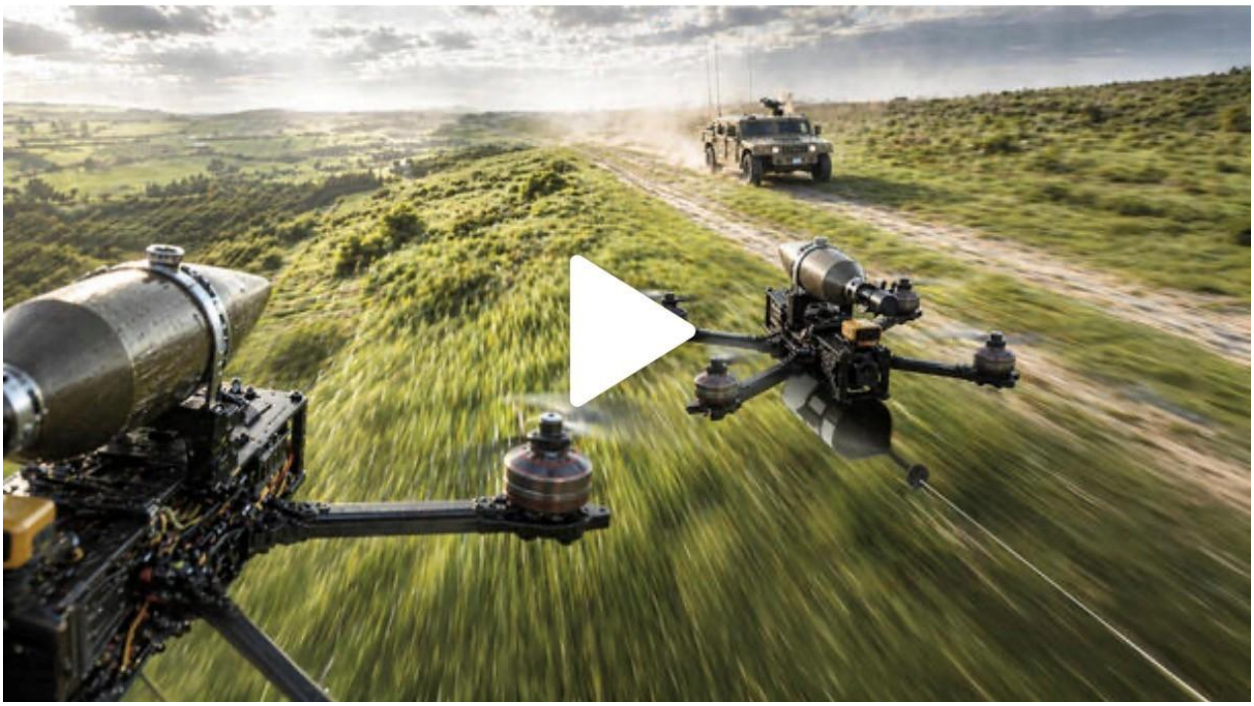
עידן הפוסט-חסימה: רחפני סיב אופטי, נשק סייבר-קינטי והפער האסטרטגי בין צה"ל לארה"ב

Article is available in English HERE



מאת: עמי אלעזרי

התפוצה המהירה של כלי טיס בלתי מאוישים בשדה הקרב המודרני חוללה שינוי משמעותי, עם המעבר מהפעלה מבוססת רדיו להנחיה באמצעות סיב אופטי פיזי. התפתחות זו עוקפת ביעילות את הדור הנוכחי של טכנולוגיות הלוחמה האלקטרונית והחסימה, ויוצרת עידן חדש של לחימה חסינת חסימות המכונה "עידן הפוסט-חסימה". המאמר הנוכחי, המבוסס על ניתוח אסטרטגי של עמי אלעזרי (CTO של 1Presale), בוחן את הארכיטקטורה הטכנולוגית של רחפנים אלו, את הקשר ההדוק לעולם הסייבר, ואת טכנולוגיית ה-Discombobulator החדשנית שהופעלה בוונצואלה.

הקשר לסייבר ואבטחת מידע

בעידן המודרני, הרחפן אינו רק כלי טיס אלא צומת ברשת (Network Node). המעבר לסיב אופטי משנה את משוואת אבטחת המידע: בעוד שהוא מונע שיבוש אלקטרומגנטי, הוא חושף סיכונים חדשים בשרשרת האספקה. שימוש ברכיבים אלקטרוניים ממקורות לא מהימנים עלול לכלול "דלתות אחוריות" המאפשרות ליריב להשתלט על הרחפן או לדלות ממנו מידע מודיעיני.

בנוסף, לוחמת הסייבר משתלבת כיום כחלק בלתי נפרד מהמענה לרחפנים. תקיפות סייבר

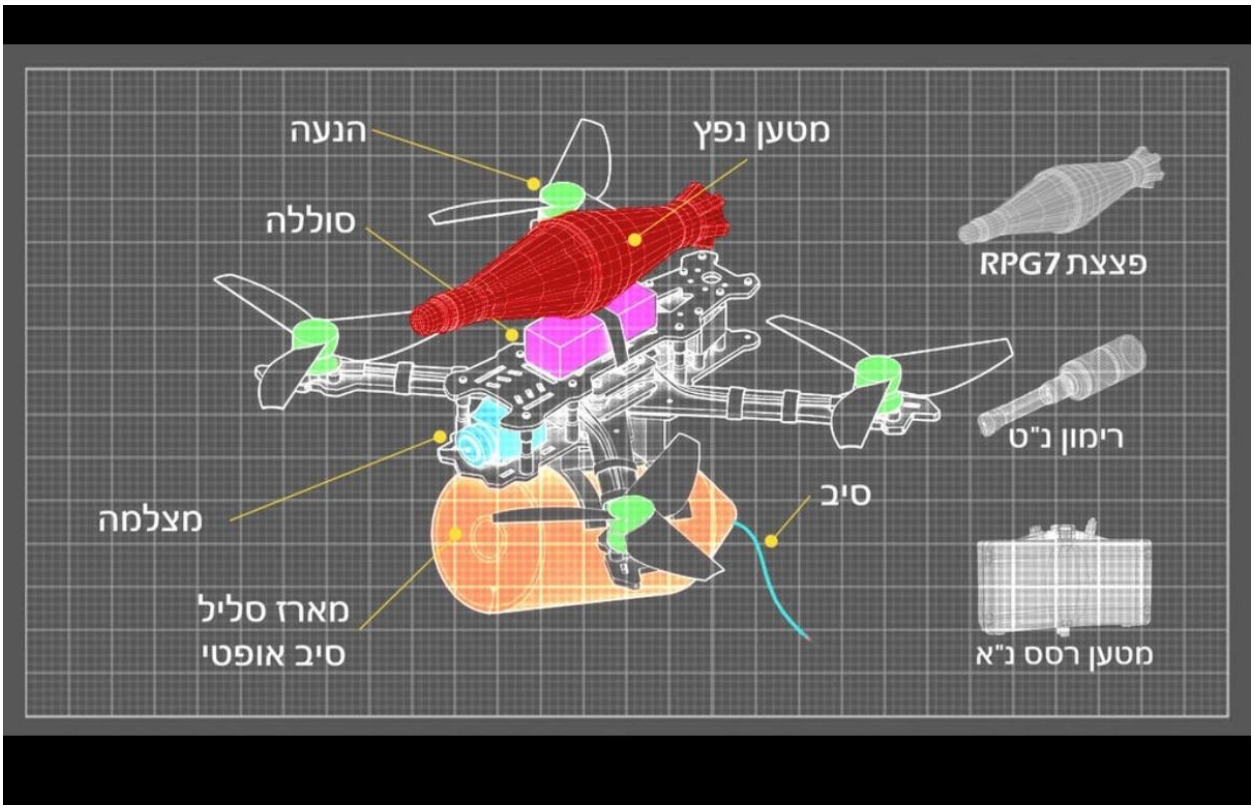
מקדימות על מערכות הבקרה (GCS) או על תשתיות SCADA המזינות את מערכי ההגנה של האויב הן קריטיות ליצירת עליונות בשטח. היכולת לשבש את התמצאות המפעיל באמצעות סייבר או שיבוש GPS רחב היקף היא נדבך מרכזי בהגנה רב-שכבתית.

נשק סייבר-קינטי: ה-Discombobulator האלקטרוני

ה-Discombobulator האלקטרוני הוא הרבה מעבר לנשק אנרגיה רגיל – הוא נשק הסייבר המתקדם ביותר של זמננו. הוא מייצג את המיזוג האולטימטיבי בין לוחמת סייבר, לוחמה אלקטרונית ואנרגיה מכוונת, ויוצר קטגוריה חדשה לחלוטין: נשק סייבר-קינטי (Cyber-Kinetic Weapon).

בניגוד להתקפות סייבר מסורתיות המתמקדות בתוכנה, הדיסקומבולטור פוגע ישירות בשכבת החומרה – מעגלים משולבים, מוליכים למחצה, שבבי זיכרון ומעבדים. פעימות ה-EMP והמיקרוגל הממוקדות שלו יוצרות "מכת ברק מלאכותית מרוכזת" החודרת דרך חריצים זעירים במארזי המכשירים. האנרגיה מייצרת קפיצות מתח אדירות המתיכות פיזית את הצמתים המיקרוסקופיים בתוך השבבים.

זהו "Cyber Hard Kill" אמיתי: המערכת לא רק מושבתת – היא נמחקת לצמיתות. שום עדכון תוכנה או גיבוי לא יכולים לשקם אותה; המטרה הופכת לגוש מתכת חסר תועלת. המערכת משתלבת עם כלי סייבר מבוססי AI לאיתור מטרות מדויק ואיסוף מודיעין על תדרי הפעלה ושרשרת הפיקוד.



פתרונות ריאליים נגד רחפני סיב אופטי בצה"ל

צה"ל מתמודד כיום עם פער משמעותי מול רחפני הנפץ של חיזבאללה, הגורמים לנזקים קשים בנפש וברכוש. במענה לשאלה איזה פתרון ריאלי ניתן ליישם, עולה צורך בשילוב שכבות:

1. **יירוט קינטי:** שימוש ברחפני יירוט (כמו יחידת Magyar Birds באוקראינה) ובתחמושת מיוחדת כגון Drone Round המפזרת חלקיקים במהירות גבוהה.
2. **פתרונות טרמיים:** שימוש ברחפני יירוט עם "חוט טיל" לוהט או חוטי חימום המסוגלים לחתוך או להמיס פיזית את הסיב האופטי (העשוי פולימר ורגיש לחום) במגע ישיר.
3. **השמדת מקור:** פגיעה ישירה בחוליות השיגור ובמפעילי הרחפנים באמצעות מודיעין סייבר וסיגינט מדויק.
4. **שיבוש מרחבי:** הפעלת משבשי GPS בכל אזור המטרה כדי להקשות על ניווט הרחפן והמפעיל כאחד.

סיכום

האיום של רחפני הסיב האופטי מחייב את צה"ל לשנות פרדיגמה – מחסימה אלקטרונית (Soft Kill) להשמדה פיזית של החומרה והסיב (Hard Kill). הפתרון הטוב ביותר הוא שילוב שכבות הכולל נשק פעימה אלקטרומגנטית ממוקד, יכולות סייבר התקפיות ויירוט קינטי פיזי.

The Post-Jamming Era: Fiber Optic Drones, Cyber-Kinetic Weapons, and the Strategic Gap Between the IDF and the US

By: Ami Elazari

The rapid proliferation of unmanned aerial systems (UAS) on the modern battlefield has introduced a significant shift from radio-frequency teleoperation to physical fiber-optic guidance. This development has effectively bypassed the current generation of electronic warfare (EW) and jamming technologies, creating a new era of "Post-Jamming" warfare. Based on strategic analysis by Ami Elazari (CTO of Presale1), this report examines the intersection of

this technology with cyber warfare and the operational gap between the IDF and the US.

Cyber and Information Security Context

Modern drones are no longer just aircraft; they are network nodes. The transition to fiber optics shifts the cybersecurity equation: while it prevents electromagnetic jamming, it exposes new risks in the supply chain. Using electronic components from untrusted sources may include "backdoors" that allow adversaries to hijack the drone or extract operational intelligence. Furthermore, offensive cyber operations are now integrated to disable the enemy's digital infrastructure, such as SCADA networks and command-and-control systems, even before physical contact occurs—a strategy known as "Left of Launch".

The New Cyber Weapon: The Electronic "Discombobulator"

The electronic Discombobulator is far more than a conventional directed-energy weapon – it is the most advanced cyber weapon of our time. It represents the ultimate fusion of cyber warfare, electronic warfare (EW) and directed-energy technology, creating an entirely new category: Cyber-Kinetic Weapon.

Unlike traditional cyber attacks that target software (viruses, ransomware, zero-days), the Discombobulator strikes directly at the hardware layer – integrated circuits, semiconductors, memory chips and processors. Its precisely focused EMP and High-Power Microwave (HPM) pulses create a "concentrated artificial lightning strike" that penetrates tiny gaps in device casings (back-door coupling), generating massive voltage spikes that physically melt microscopic junctions inside the chips.

This is true cyber Hard Kill: the system is not merely disabled – it is permanently erased. No software patch, no backup, no recovery is possible. The target becomes a useless lump of metal. It integrates seamlessly with AI-driven target acquisition and preliminary cyber attacks that temporarily blind electronic defenses.

Realistic Solutions for the IDF Against Fiber-Optic Drones

The IDF currently lacks a comprehensive operational response to fiber-optic drones, which have caused casualties among soldiers and civilians. Realistic solutions include:

1. **Kinetic Interception:** Utilizing interceptor drones (modeled after Ukraine's "Magyar Birds") and specialized "Drone Round" ammunition that disperses particles at high velocity.
2. **Thermal Solutions:** Interceptor drones equipped with heated filaments or "missile wires" that can physically cut or melt the polymer fiber link upon contact.
3. **Cyber & Signal Jamming:** Deploying wide-scale GPS jamming to confuse the operator's orientation and using cyber-intelligence to strike drone operator units directly.
4. **Physical Obstacles:** Implementing tactical improvements such as specialized netting and high-altitude observer networks.

Conclusion

The fiber-optic drone threat requires a paradigm shift from "soft" electronic jamming to "hard" physical and hardware-level destruction. Israel must bridge the operational gap by investing in focused electromagnetic pulse (EMP) technologies and offensive cyber integration to ensure battlefield superiority in the post-jamming era.