# مزایای عملیاتی استفاده از جنگ الکترونیک سایبری (CEW) در میدان نبرد

**حامد شیروی**[*۱]

۱- مربی دانشکده فنی مهندسی، دانشگاه افسری و تربیت پاسداری امام حسین(ع)-hshiravi@ihu.ac.ir

**چکیده:**

در حالی که فضای سایبری به عنوان یک میدان نبرد جدید در حال ظهور است، روش‌ها و کاربردهای جنگ الکترونیک متعارف احتمالاً تغییر خواهد کرد. مفهوم جنگ الکترونیک سایبری که قابلیت‌های فضای سایبری را با روش‌های سنتی EW[۲] ادغام می‌کند، شکل جدید و پیشرفته‌ای از حمله الکترونیکی است. در این مقاله بر حوزه فضای سایبری میدان نبرد تأکید شده و امکان ادغام مفهوم CW[۳] در اقدامات EW مورد بررسی قرار گرفته است. از روش تحلیل SWOT[۴] (نقاط قوت، ضعف، فرصت‌ها و تهدیدها) برای بیان مزایای عملیاتی استفاده از مفهوم CEW در میدان جنگ استفاده می‌شود. مزایای عملیاتی CEW با استفاده از اثرات آن بر سیستم‌های دفاع هوایی دشمن، شبکه‌های ارتباطی و سیستم‌های اطلاعاتی مورد تحلیل قرار می‌گیرد. در نهایت، مقایسه مفهوم CEW و کاربردهای EW ، به این موضوع می‌انجامد که استفاده از مفهوم CEW در میدان جنگ امکان‌پذیر است و ممکن است مزایای عملیاتی مهمی را به‌همراه داشته باشد. اگرچه رایانه‌های سیستم‌های نظامی توسعه‌یافته پیچیده‌تر از رایانه‌های معمولی هستند، امّا از آن جایی که سیستم‌های بسته هستند، در معرض تهدیدات سایبری قرار نمی‌گیرند. این مفهوم قصد دارد نشان دهد که این سیستم‌های بسته در برابر تهدیدات سایبری نیز باز هستند. در نتیجه، تجزیه و تحلیل SWOT، مفهوم CEW نیروی هوایی را برای استفاده مؤثر در عملیات سایبری فراهم می‌کند. از سوی دیگر، از آن جا که معیارهای خسارت وثیقه آن (CDC[۵]) کم است، به نظر می‌رسد استفاده از سیستم‌های حمله الکترونیکی سایبری رو به افزایش است.

**کلید واژه‌ها:** جنگ سایبری، جنگ الکترونیک، جنگ الکترونیک سایبری، فضای مجازی.

## Operational Advantages Of Using Cyber Electronic Warfare (CEW) In The Battlefield

**Hamed Shiravi**[*۱]

**Lecturer, Faculty of Engineering, Imam Hossein Officer and Guard Training University - hshiravi@ihu.ac.ir**

**Abstract**

While cyberspace is emerging as a new battlefield, conventional Electronic Warfare (EW) methods and applications are likely to change. Cyber Electronic Warfare (CEW) concept which merges cyberspace capabilities with traditional EW methods, is a new and enhanced form of the electronic attack. In this study, cyberspace domain of the battlefield is emphazised and the feasibility of integrating Cyber Warfare (CW) concept into EW measures is researched. The SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis method is used to state the operational advantages of using CEW concept in the battlefield. The operational advantages of CEW are assessed by means of its effects on adversary air defense systems, communication networks and information systems. Outstanding technological and operational difficulties are pointed out as well. As a result, a comparison of CEW concept and conventional EW applications is presented. It is concluded that, utilization of CEW concept is feasible at the battlefield and it may yield important operational advantages. Even though the computers of developed military systems are less complex than normal computers, they are not subjected to cyber threats since they are closed systems. This concept intends to show that these closed

[۱] Cyber Electronic Warfare

[۲] Electronic Warfare

[۳] Cyber Warfare

[۴] Strengths, Weaknesses, Opportunities and Threats

[۵] Collateral Damage Criteria

systems are also open to the cyber threats. As a result of the SWOT analysis, CEW concept provides Air Forces to be used in cyber operations effectively. On the other hand, since its Collateral Damage Criteria (CDC) is low, the usage of cyber electronic attack systems seems to grow up.

**Keywords:**Cyber war, electronic war, cyber electronic war, virtual space.

**۱- مقدمه**

پس از عملیات طوفان صحرا (۱۹۹۱م) با کمک اینترنت، که در آن برای اولین‌بار سیستم‌های ارتباطی ملّی در برنامه‌های عملیاتی هدف قرار می‌گرفت، اینترنت، بسیار سریع گسترش یافت. جنگ سایبری به عنوان یک مفهوم جدید شروع به ظهور کرده است. از سوی دیگر، در جنگ دوّم خلیج فارس، مزایای استفاده از فناوری در منطقه عملیاتی به وضوح دیده شد و تکنیک‌های جدید مرتبط با جنگ سایبری شروع به توسعه کردند.

در سال ۲۰۰۷م، استونی، یکی از کشورهای پیشرو اروپا که دولت الکترونیک را در اروپا اِعمال کرد، در معرض اوّلین حمله سایبری سیستماتیکی توسط روسیه قرار گرفت[۱]. حمله سایبری روسیه به گرجستان در طول جنگ اوستیای جنوبی در سال ۲۰۰۸م را می‌توان به عنوان حمله سایبری جنبشی توصیف کرد؛ زیرا این حمله در یک جنگ متعارف رُخ داده است. استاکس‌نت، حمله دیگری است که در سال ۲۰۱۰م علیه نیروگاه‌های هسته‌ای ایران رُخ داد، حادثه مهمی بود که آشکارا تأثیر سلاح سایبری توسعه‌یافته را برای یک هدف خاص نشان می‌داد[۲].

علاوه بر این، لاکهید مارتین، یک شرکت پیشرو در ارائه‌ی تسلیحات، اعلام کرد که در معرض حمله سایبری قرار گرفتند و در سال ۲۰۱۱م با انجام اقدامات احتیاطی از سیستم خود با موفقیت دفاع کردند. این حمله شبکه قابلیت‌های CW [۳] را برجسته می‌کند. می‌توان گفت که حملات سایبری اخیر متوجه شرکت‌های دفاعی بوده است. با توجه به اینکه این حملات برای دست‌یابی به اطلاعات سیستم تسلیحاتی است، می‌توان آنها را به عنوان حملات سایبری غیرمستقیم به سیستم‌های نظامی توصیف کرد. در نتیجه، به تدریج CW خود را به یک راه بی‌خون امّا مؤثر برای جنگ به‌ویژه علیه کشورهای توسعه‌یافته که هدف سایر کشورها در مورد حمله سایبری هستند، تبدیل کرد.

جنگ الکترونیک با استفاده از سیستم‌های راداری به عنوان دفاع هوایی در جنگ جهانی دوّم پدیدار شد. هنگامی که موشک‌های هدایت‌شونده به کمک رادار باعث تلفات هواپیماهای زیادی در ویتنام شد، EW به تدریج در جنگ‌های بعدی مانند جنگ خلیج فارس، جنگ کوزوو، کارایی خود را افزایش داد و همچنان به یکی از مهم‌ترین عوامل در میدان جنگ تبدیل شد.

به عنوان سیستم‌های تسلیحاتی مورد استفاده در میدان عملیات، می‌توان در نظر گرفت که جنگ الکترونیک علاوه بر باندهای فرکانس رادیویی و راداری، باندهای مادون قرمز، مرئی و فرابنفش را در طیف الکترومغناطیسی نیز پوشش می‌دهد. بنابراین، می‌توان نتیجه گرفت که EW بر روی مبارزه در تمام مراحل تأثیر می‌گذارد[۴].

رابطه بین CW و EW را می‌توان به عنوان رابطه بین جنگ نامتقارن و متقارن در نظر گرفت. برخلاف CW، هدف EW جلوگیری از انتقال اطلاعات با اقدام تقریباً بدون در نظر گرفتن اهداف خاص است. CW به عملیاتی می‌پردازد که شامل اهداف خاص‌تر و اطلاعات دیجیتالی می شود[۵]. در حالی که فضای سایبری به عنوان جنگ نامتقارن در حال ظهور است، روش‌ها و کاربردهای رایج EW قدیمی و کافی نیستند. بنابراین، علاوه بر استفاده از طیف الکترومغناطیسی، باید تکنیک‌های جدیدی برای حمله و دفاع از شبکه‌ها، سیستم‌های ارتباطی و سیستم‌های الکترونیکی ایجاد شود.

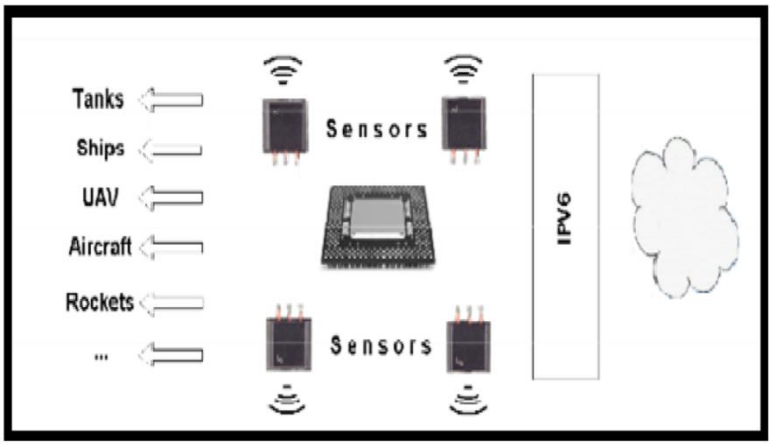
با توجه به دلایل یادشده در بالا، برنامه‌ریزان عملیات آینده، بر استفاده از CW و EW با هم تأکید دارند. در نتیجه، این مطالعه به بررسی جنگ الکترونیک سایبری می‌پردازد. در جنگ سایبری از روش‌ها و برنامه‌های کاربردی CW و EW با هم و متفاوت از هر یک از آنها، از نظر استفاده از اهداف حمله بهره می‌برند. در این مرحله می‌توان ادّعا کرد که مفهوم CEW شکل جدید و پیشرفته‌ای از حمله الکترونیکی و حاوی عناصر جنگ سایبری است. در واقع، این دگرگونی حمله الکترونیکی به دلیل وابستگی روزافزون به شبکه‌ها، اینترنت و سیستم‌های ارتباطی تقریباً اجتناب‌ناپذیر است.

**۲- دامنه فضای مجازی در منطقه نظامی**

قبل از صحبت در مورد مفهوم CEW، لازم است حوزه فضای سایبری را بررسی کنیم تا به عمق فضای سایبری و تأثیرات جنگ سایبری در میدان نبرد پی ببریم و خطرات آن را بهتر تحلیل کنیم. با توجه به این هدف، یکی از بهترین توصیف‌های فارنکروگ این است که: «طیف وسیعی از افکار در مورد وسعت فضای مجازی یا آنچه باید در CW گنجانده شود، وجود دارد. یک پاسخ معمولی به فضای سایبری چیست؟ معمولاً شامل توصیفی از شبکه‌های رایانه‌ای یا اینترنت است. با این حال، تعریف ارتش از فضای سایبری، اذعان دارد که فضای سایبری چیزی بیش از این شبکه‌های رایانه‌ای است. مهم‌تر از آن، از آنجایی که سیستم‌های شبکه‌ای از طریق استفاده از انرژی الکترومغناطیسی ایجاد می‌شوند، جنگ در فضای سایبری لزوماً شامل قابلیت هایی است که در حال حاضر جنگ الکترونیک محسوب می شود. حتی شبکه‌هایی که مستقیماً به اینترنت متصل نیستند، ممکن است با استفاده از انرژی الکترومغناطیسی برای بازجویی یا اختلال در اجزای الکترونیکی شبکه مورد حمله قرار گیرند. این یک تمایز مهم برای ارتش است»[۶].

در این بخش، سعی می‌شود این تمایز مهم برای نظامیان مشخّص شود. از این رو، می‌توان گفت که حوزه‌ی فضای سایبری شامل سیستم‌های EW است که از طیف الکترومغناطیسی، سیستم‌های الکترونیکی و زیرساخت‌های فیزیکی در سیستم‌های نظامی استفاده می‌کند. این رابطه توسط AFDD 2-11 حاوی تعامل بین حوزه فیزیکی و فضای مجازی به شرح زیر توضیح داده شده است: «فضای مجازی، داده‌ها را ذخیره، اصلاح و مبادله می‌کند. از الکترونیک و انرژی الکترومغناطیسی به منظور انجام این تغییر و تبادل استفاده می شود که اتصال شبکه‌ای را ایجاد و داده‌ها را مبادله می‌کند. این همه توسط زیر ساخت فیزیکی فعال می شود که شامل تجهیزاتی مانند آنتن‌ها، روترها، سوئیچ‌ها، خطوط انتقال و کابل‌های فیبر نوری است. حوزه‌ی فضای سایبری از طیف الکترومغناطیسی (EMS) برای ذخیره، انتقال و اصلاح داده‌ها در زیر ساخت‌های مناسب استفاده می کند»[۷].

فعالیت‌هایی مانند ذخیره‌سازی داده‌ها، اصلاح و تبادل با ایجاد شبکه بینابین سیستم‌ها ممکن است برنامه‌هایی باشد که در CW از آنها استفاده می‌شود. بنابراین، دارایی‌هایی که از فناوری و سیستم‌های رایانه‌ای در سطوح استراتژیک، عملیاتی و تاکتیکی استفاده می‌کنند، به‌ویژه در مراکز فرماندهی و کنترل، نیروی هوایی ارتش و نیروی دریایی مورد استفاده در میدان نبرد می‌توانند در معرض خطر حملات سایبری قرار گیرند. ادغام سیستم‌های نظامی می‌تواند خطرات سایبری بیشتری در میدان نبرد داشته باشد. در حقیقت، بسیاری از شبکه‌های فرماندهی و کنترل نظامی و سامانه‌های پدافند هوایی، شبکه‌های ایزوله یا بسته هستند که مستقیماً قابل دسترسی نیستند. امّا، تمام سیستم‌های نظامی با اطلاعات فشرده، همان طور که در شکل ۱ ارائه شده است، به قابلیت‌های پردازش اطلاعات، ارتباطات و حس‌گر در میدان نبرد مجهز خواهند شد[۸]. با توجه به این موضوع، ما باید تهدیدات سایبری برای ارتش یا در میدان جنگ را نه تنها با شبکه‌ها، بلکه با شبکه‌های بسته و انرژی الکترومغناطیسی مورد انتقاد قرار دهیم.




شکل (۱): سیستم‌های نظامی با اطلاعات فشرده در معرض تهدید[۸].

تعریف نظامی CW، ترکیبی از حمله شبکه کامپیوتری و دفاع شبکه کامپیوتری و احتمالا عملیات اطلاعاتی ویژه است[۹]. به منظور درک CW، تفاوت بین جنگ متعارف و CW در جدول ۱ ارائه شده است.

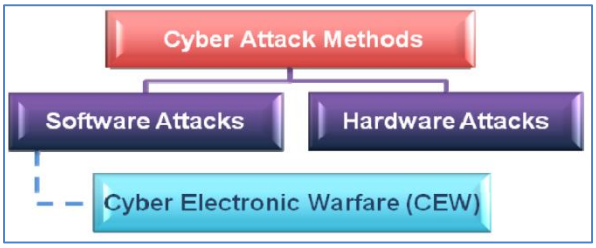
جدول (۱): تفاوت بین جنگ متعارف و جنگ سایبری[۱۰].

| شاخص | جنگ متعارف | جنگ سایبری |
|---|---|---|
| منبع حمله | به‌راحتی می‌توان منبع را پیدا کرد | یافتن منبع بسیار دشوار است |
| سرعت | سرعت هواپیما، تانک یا سیستم تسلیحاتی هم همین‌طور | با سرعت نور |
| اثر | در ناحیه فیزیکی مؤثر است | بیشتر در مورد سیستم‌های اطلاعات و ارتباطات (ICS)، امّا هم‌چنین اثرات جانبی در حوزه فیزیکی |
| طرفین | بین دو یا چند نیروی مسلح | یک فرد، یک گروه، یک سازمان یایک کشور |
| هزینه | بستگی به هزینه سیستم‌های تسلیحاتی دارد | بسیار ارزان، حتی یک کامپیوتر نیز می‌تواند کافی باشد |
| سلاح‌ها | سلاح‌های متعارف | تراشه‌ها و سایر سخت‌افزارها و نرم‌افزارهای مورد استفاده در سیستم‌های کامپیوتری |
| الزامات فناوری | به تکنولوژی پیشرفته نیاز دارد | فناوری پیشرفته مورد نیاز نیست، امّا فناوری پیشرفته می‌تواند اثربخشی را افزایش دهد |
| نشانه‌های حمله | امکان تشخیص | عمدتاً تشخیص آن سخت است |
| تشخیص آسیب | تشخیص آسان آسیب با توجه به اثر فیزیکی جنگ | تشخیص نتایج حمله تقریباً غیرممکن است |

به موازات آن، تفاوت معیارهای CW ارائه‌شده در جدول را می‌توان به عنوان ویژگی‌های نامتقارن CW ارزیابی کرد. همان طور که در جدول ۱ ارائه شده است، استفاده از روش‌های CW مؤثرتر از استفاده از روش‌های جنگ متعارف خواهد بود، زیرا سلاح‌های سایبری ارزان‌تر، نامرئی و غیرقابل شناسایی هستند. بنابراین، کشورهایی که در حال توسعه سلاح‌های سایبری هستند ممکن است فقط از روش‌های CW استفاده کنند یا از تلاش‌های جنگ متعارف از طریق سلاح‌های سایبری در میدان نبرد حمایت کنند. خصوصاً داشتن قابلیّت حمله سایبری در میدان نبرد، در کنار روش‌های جنگی متعارف، می‌تواند اقتصاد نیرو را فراهم کند.

### ۳ – روش‌های حمله سایبری در میدان نبرد

روش‌های حمله سایبری قابل استفاده در میدان نبرد را می‌توان در دو گروه «حملات نرم‌افزاری» و «حملات سخت‌افزاری» بررسی کرد. همه‌ی حملات سایبری چه نرم‌افزاری و چه سخت‌افزاری، سعی می‌کنند با استفاده از شبکه‌های سیمی یا بی‌سیم، سیستم هدف را کاملاً دست‌کاری یا نابود کنند.




شکل (۲): روش‌های حمله سایبری در میدان نبرد.

همان طور که در شکل ۲ ارائه شده است، مفهوم CEW ممکن است به عنوان روشی برای حملات نرم افزاری تعیین شود. همه روش‌های حمله سایبری از سلاح‌های سایبری متغیر استفاده می‌کنند. بر این اساس، تهدیدات سایبری احتمالی برای میدان نبرد تعیین شده و سلاح‌های سایبری در جدول ۲ نشان داده شده است.

جدول (۲): تهدیدات سایبری احتمالی در میدان نبرد.

| روش‌های حمله سایبری | سلاح‌های سایبری |
|---|---|
| حملات نرم‌افزاری | بدافزار |
| | نرم‌افزارهای جاسوسی |
| | بمب ساعتی سایبری |
| | سیستم حمله جنگ الکترونیک سایبری |
| حملات سخت‌افزاری | ریزتراشه‌ها |
| | سلاح‌های مایکروویو با قدرت بالا |
| | طوفان |
| | نانو مکانیک |

همان طور که در جدول ۲ ارائه شده است، CW نوع جدیدی از سلاح با اثرات مختلف آن بر روی یک هدف است. علاوه بر سلاح‌هایی که به عنوان یک سلاح سایبری ساخته شده‌اند، برخی از سلاح‌های دیگر که برای توسعه به عنوان یک سلاح سایبری در نظر گرفته نشده بودند، کاندیدای حضور در زرادخانه هستند. به عنوان مثال، اگرچه آنها هنوز در دوره ارتقا هستند، سلاح‌های حمله سخت‌افزاری را می‌توان سلاح‌های سایبری آینده در نظر گرفت. این سلاح‌ها: ریزتراشه‌ها (CTB برای سخت‌افزار)، HPMW (بمب‌های پالس الکترومغناطیسی: بمب‌های الکترونیکی)، TEMPEST (سلاح‌های جاسوسی سایبری برای حملات سخت‌افزاری) و نانومکانیک (قطعات مکانیکی بسیار کوچک که به‌راحتی می‌توانند به سیستم‌های الکترونیکی تزریق شوند) هستند.

بدافزارها (ویروس‌های کامپیوتری، کرم‌ها، تروجان‌ها)، جاسوس افزارها، CTBها (بمب منطقی و دروازه‌های تله) و سیستم حمله CEW سلاح‌های سایبری هستند که نرم‌افزار را هدف قرار می‌دهند. در حال حاضر، بیشتر حملات نرم‌افزاری بر سیستم‌های غیرنظامی و نظامی تأثیر می‌گذارد. با این حال، آگاهی از این حملات بسیار دشوار است زیرا سلاح‌های سایبری آنها پس از داشتن مکان‌هایشان در سیستم‌ها قابل شناسایی نیستند. حملات اخیر با هدف قرار دادن رایانه‌های مأموریت تسلیحات نیروی هوایی نشان می‌دهد که اهداف این حملات نه تنها سرقت اطلاعات بلکه تأثیرگذاری بر سیستم در حال اجراست. برای تأثیرگذاری بر سیستم در حال اجرا، CTBها نیز به‌راحتی قابل استفاده هستند. آنها را می‌توان در مناطق آسیب‌پذیر شناسایی‌شده در زمان صلح قرار داده و در زمان جنگ فعال کرد. در این بخش، جایگاه سیستم CEW در روش‌های

حمله سایبری به اختصار نشان داده شده است. از آن جایی که سیستم حمله CEW استفاده از نیروی هوایی در جنگ سایبری را برجسته می‌کند، مفهوم حمله CEW در بخش دیگری به تفصیل توضیح داده شده است.

### ۴- نیروی هوایی در جنگ سایبری

با بررسی حملات سایبری که قبلاً ذکر شد، بدیهی است که هیچ یک از آنها به طور مستقیم بر زندگی خصوصی ما تأثیر **نمی‌گذارند**، امّا با توجه به حملات سایبری احتمالی در آینده، ممکن است به دلیل افزایش تعداد رایانه‌ها و نیاز به سیستم‌های کنترل رایانه، به شدت گسترش یابد؛ مانند بسیاری از فعالیت‌ها و سیستم‌های دولتی، سیستم‌های نظامی به طور فزاینده‌ای به فناوری و فضای سایبری وابسته هستند. در میان سیستم‌های نظامی، سیستم‌های مربوط به نیروی هوایی بیش‌ترین درصد پلت‌فرم‌های مُبتنی بر فناوری را دارند.

سیستم‌های تسلیحات هوایی نیز به طور فزآینده‌ای به نرم‌افزار، سخت‌افزار رایانه و شبکه‌های میدان نبرد وابسته هستند و بنابراین، می‌توانند از طریق سیستم‌های سایبری مورد هدف قرار گیرند. در حالی که امنیّت این سیستم‌های تسلیحاتی همگام با توسعه و پیاده سازی فناوری سایبری پیشرفت می‌کنند، می‌توانند به طور فزآینده‌ای تحت تأثیر حملات سایبری قرار گیرند (جدول ۳)[۱۱].

جدول (۳): وابستگی‌های نرم‌افزاری سکوهای هوایی[۱۱].

| هواپیما | سال | درصد توابع نرم‌افزار |
|---|---|---|
| F-4 | ۱۹۶۰ | ۸ |
| A-7 | ۱۹۶۴ | ۱۰ |
| F-111 | ۱۹۷۰ | ۲۰ |
| F-15 | ۱۹۷۵ | ۳۵ |
| F-16 | ۱۹۸۲ | ۴۵ |
| B-2 | ۱۹۹۰ | ۶۵ |
| F-22 | ۲۰۰۰ | ۸۰ |

همان طور که در جدول ۳ ارائه شده، مشخص شده است که نیروهای نظامی به‌ویژه واحدهای نیروی هوایی از این حملات احتمالی تحت تأثیر سکوهای هوایی شامل شبکه‌ها، سیستم‌های دیجیتال، زیرساخت‌ها و هر عنصر دیگری که به عنوان اطلاعات، ارتباط و یا عمل می‌کند، متأثر خواهند شد. سیستم‌های کنترل. مثلاً؛ جنگنده‌های فرانسوی رافال در ژانویه ۲۰۰۹م به دلیل یک کرم ویندوز مایکروسافت که برخی از نرم افزارهای سیستم‌های پشتیبانی زمینی را آلوده کرده بود، زمین‌گیر شدند[۱۲]. در این مثال، عفونت کرم کاملاً تصادفی است. در صورت عمدی بودن و در حین آماده‌سازی مأموریت عملیاتی مهم، کارآیی هواپیما کاهش می‌یابد. در چنین مواردی، مأموریت‌های پروازی برنامه‌ریزی شده را نمی‌توان لزوماً در میدان جنگ انجام داد. مثال مهم دیگر، در مورد ماهواره‌ها است. بر اساس پیش‌نویس گزارش کمیسیون بازبینی اقتصادی و امنیتی ایالات متحده و چین، ماهواره Terra EOS AM-1 ناسا که برای مطالعه تغییرات آب و هوایی و محیطی استفاده می‌شد، در اکتبر ۲۰۰۸م، ۹ دقیقه یا بیشتر تداخل را تجربه کرد که توسط دیفنس نیوز به دست آمد[۱۳]. اگر یک مهاجم سایبری ماهواره‌ای را به عنوان هدف انتخاب کند، می‌تواند زیرساخت‌ها و سیستم‌های حیاتی در میدان نبرد را نیز به عنوان هدف انتخاب کند. به همین ترتیب، سیستم‌های هواپیمای بدون سرنشین (UAS) نیز می‌توانند از طریق جنگ سایبری مورد هدف دشمنان قرار گیرند. مثلاً؛ یک UAS حواصیل که ۸۰-۹۹ درصد وابستگی به نرم‌افزار دارد، مأموریت SAR خود را (شامل برخاستن/ فرود) تنها با فشار دادن دو دکمه در اتاق کنترل انجام می‌دهد.

جدول (۴): زیرساخت‌ها و سیستم‌های حیاتی برای نیروی هوایی.

| ردیف | سیستم‌ها |
|---|---|
| ۱ | سیستم‌های C4ISR |
| ۲ | سیستم‌های پیوند داده |
| ۳ | سیستم‌های دفاع هوایی |
| ۴ | هواپیما |
| ۵ | UASها |
| ۶ | سیستم‌های تسلیحاتی |
| ۷ | امکانات فرودگاه |
| ۸ | سیستم‌های الکتریکی |

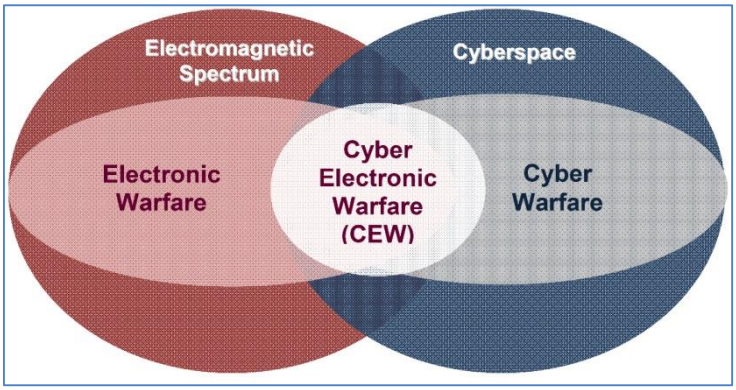
سیستم‌های جدول ۴ به عنوان برخی از زیرساخت‌ها و سیستم‌های حیاتی برای نیروی هوایی تعیین شده‌اند. همان‌گونه که مشاهده می‌شود، اکثر سیستم‌های نیروی هوایی به نرم‌افزار وابسته هستند. بنابراین، دفاع از این سیستم‌ها با روش‌های متعارف کافی نیست. از این‌رو، به‌دست آوردن قابلیّت حمله سایبرییا ضد حمله سایبری در کنار دفاع سایبری برای بقای دارایی‌های نیروی هوایی بسیار مهم است. در این زمینه، این مطالعه CEW را به عنوان یک روش حمله سایبری پیشنهاد می‌کند که از دامنه سایبری به منظور تولید شکل پیشرفته‌تری از حمله الکترونیکی استفاده می‌کند.

### ۵- مفهوم جنگ الکترونیک سایبری

CW و EW ابتدا با هم در جنگ بین روسیه و گرجستان در سال ۲۰۰۸ مورد استفاده قرار گرفتند. قبل از عملیات، برخی از مهاجمان سایبری رو سی (یا هکرها) CW را علیه گرج ستان از جمله سی ستم‌های غیرنظامی با م سدود کردن ب سیاری از وب سایت‌ها و تغییر زمینه آنها آغاز کردند. پس از این اقدامات، عملیات نظامی آغاز شد[۱۴]. اگرچه این اقدامات بین رو سیه و گرجستان CW نامیده می‌شود، یکCW واقعی هنوز اتفاق نیفتاده است. شکل CW آینده‌نگر مشخص نیست، امّا تصور می‌شود که سلاح‌های سایبری فعلی، سلاح‌های سایبری احتمالی و حتی سلاح‌های سایبری شدید در اولین CW آینده استفاده خواهند شد.

مطالعات نشان می‌دهد که اگرچه اثرات حملات سایبری در استفاده غیرنظامی شدید است، امّا نتایج آن کشنده نیست. گام بعدیCEW با پشتیبانی از تسلیحات متعارف است. قرار است از طیف الکترومغناطیسی و فناوری اطلاعات در جنگ‌ها استفاده شود و کسی که این قدرت را داشته باشد اثرات دلخواه را ایجاد می‌کند. از آن جایی که مطالعات در این زمینه بسیار محرمانه است، جزئیات آن فاش نمی شود. با این وجود، مشخص است که کشورهای توسعه یافته در این زمینه کار می کنند.

تحلیل‌گران از ایالات متحده تأکید می‌کنند که مبارزه با چریک‌های سایبری غیرنظامی بسیار دشوار است. صاحب‌نظران بر این نظرند که د ستگاه‌های جنگ الکترونیکی می‌تواند سی ستم‌های SAM معمولی را به‌راحتی کنترل کند، امّا نکته چالش برانگیز شنا سایی تروریـ ستها و تحت تأثیرقرار گرفتن واحدهای کنترل ا ست. به دلیل ضعف امنیتی نا شی از شبکه‌های بی سیم، اطلاعات در معرض پارگی هستند. حتی اگر سیستم‌های نظامی نرم‌افزار رمزنگاری بسیار قابل اعتمادی دارند، می‌توان این سیستم‌ها را مسدود کرد.




شکل (۳): مفهوم CEW.

همان طور که در شکل ۳ ارائه شده است، در حالی که جنگ الکترونیک از طیف الکترومغناطیسی استفاده می‌کند و CW از عناصر فضای سایبری استفاده می‌کند، جنگ الکترونیک سایبری استفاده یکپارچه از همه‌ی این عناصر را پیشنهاد می‌کند. مطالعات درباره سیستم‌های حمله CEW هنوز در مراحل اولیه خود هستند، امّا برخی از آنها در حال توسعه هستند. به عنوان مثال، نیروی دریایی ایالات متحده سلاحی به نام مختل‌کننده نسل بعدی تولید کردند. برخلاف سیستم‌های نسل قدیم EW، این سلاح سایبری اطلاعات را توسط دستگاهی مانند رادار تولید می‌کند و به‌روشی الگوریتمی انتقال می‌دهد[۱۵]. رویه‌های حمله الکترونیک سایبری که در سکوهای هوایی مورد استفاده قرار می‌گیرد را می‌توان به طور خلاصه و به شرح زیر فهرست کرد:

- ترسیم نقشه شبکه دشمن توسط حس‌گر
- تشخیص دقیق محل آنتن شبکه
- تولید بسته اطلاعاتی شامل الگوریتم با استفاده از آرایه اسکن الکترونیکی
- نفوذ به شبکه هدف با دسترسی به آنتن مناسب

با استفاده از این مراحل می‌توان به آنتن هدف نفوذ کرد. این روش‌های حمله‌ی سایبری می‌توانند سیستم ارتباطی دشمن را به روش‌های مختلفی تحت تأثیر قرار دهند: گوش دادن، تغییر ارتباطات آنها یا از بین بردن کامل سیستم آنها[۱۴].

برای بیان شفاف این موضوع باید حمله الکترونیکی که رُکن EW است با حمله الکترونیک سایبری مقایسه شود. در حمله الکترونیکی، رادار هدف گیر می‌کند و سیگنال پارازیت می‌تواند به طور مداوم ارسال شود. از طرفی در حمله الکترونیکی سایبری می‌توان پردازنده‌ی مرکزییک سیستم الکترونیکی را به عنوان هدف انتخاب کرد. هدف اصلی ارسال جریان داده به پردازنده سیستم هدف است. برای موفقیت در این فرآیند زمانی که با حمله الکترونیکی متفاوت است، کافی است. نکته دیگر این است که حمله الکترونیکی را می‌توان شناسایی کرد و دشمنان می‌توانند اقدامات احتیاطی مختلفی را انجام دهند در حالی که تشخیص حمله الکترونیکی سایبری تقریباً غیرممکن است. حتی اگر حمله الکترونیکی سایبری شناسایی شود، ممکن است برای انجام اقدامات احتیاطی در برابر آن دیر باشد.

جدول (۵): مقایسه EW معمولی و CEW.

| EW متعارف | CEW |
|---|---|
| مداوم | ممکن است یک حمله کافی باشد |
| قابل تشخیص | تشخیص مشکل است |
| تا حدی مؤثر است | کاملاً مؤثر |
| نیاز به هوش در مورد هدف | به اطلاعات دقیق در مورد هدف نیاز دارد |

| | |
|---|---|
| بخشی از یک سیستم را هدف قرار می‌دهد | سیستم عصبی مرکزی را هدف قرار می‌دهد |
| از طیف الکترومغناطیسی استفاده می‌کند | از فضای مجازی از طریق طیف الکترومغناطیسی استفاده می‌کند |
| جلوه محدودی ایجاد می‌کند | تمام جلوه‌های مورد نظر را ایجاد می‌کند |
| قادر به نفوذ به هدف | برای نفوذ به هدف باید بر چالش‌های امنیتی غلبه کرد |

نرم‌افزار CEW بر منطق سیستم عامل تجهیزات دفاع هوایی دشمن تأثیر می‌گذارد. یک حمله موفقیت‌آمیز CEW ممکن است باعث شود که سیستم عامل خود را چیز دیگری احساس کند. به منظور واقع بینانه‌تر، می‌توان ادّعا کرد که نرم‌افزاری که به سیستم عامل هدف تزریق می‌شود، می‌تواند چیزی را ایجاد کند که بدیهی است دشمن انتظارش را ندارد. در واقع، سیستم‌های نظامی توسعه یافته طوری طراحی شده‌اند که بسیار ساده و سریع عمل کنند. حتی اگر رایانه‌های سیستمی آنها نسبت به رایانه‌های معمولی کارآیی کمتری دارند، امّا از آن‌جایی که سیستم‌های بسته هستند، در معرض تهدید قرار نمی‌گیرند. این مفهوم قصد دارد چنین سیستم‌های بسته‌ای را در برابر تهدیدات آسیب‌پذیر کند.

در حالی که مفهوم CEW در حال پیشرفت است، نرم‌افزار جدید برای برنامه‌های کاربردی CEW در حال ایجاد است. برنامه کامپیوتری Suter، یک سیستم حمله شبکه هوابرد، می‌تواند به عنوان مثال برای این مورد ذکر شود. Suter یک برنامه کامپیوتری نظامی است که توسط BAE Systems (شرکت هوافضا و دفاع بریتانیا) توسعه یافته و به شبکه‌های کامپیوتری و سیستم‌های ارتباطی متعلق به دشمن حمله می‌کند. این متخصص برای تداخل با رایانه‌های سیستم‌های یکپارچه دفاع هوایی است. سه نسل از Suter توسعه یافته است. Suter-1 به اپراتورهای خود اجازه می‌دهد تا آنچه را که اپراتورهای رادار دشمن می‌توانند ببینند، نظارت کنند. Suter-2 به آنها اجازه می‌دهد کنترل شبکه‌های دشمن را در دست بگیرند و حسگرهای آنها را هدایت کنند. Suter-3 که در تابستان ۲۰۰۶ آزمایش شد، امکان تهاجم به اهداف حساس زمانی مانند پرتابگرهای موشک بالستیک میدان نبرد یا پرتابگرهای متحرک موشک زمین به هوا را فراهم می‌کند.این برنامه با هواپیماهایی مانند EC-130، RC-135 و F-16CJ آزمایش شده است[۱۶].

### ۶- تجزیه و تحلیل SWOT مفهوم CEW

علاوه بر مزایای عملیاتی CEW در میدان نبرد، می‌توان از آن به عنوان تابعی از نیروی هوایی در آینده نیز استفاده کرد. بنابراین، نیروی هوایی برای CW بسیار مهم و مؤثر خواهد بود. در این تحقیق از روش تحلیل SWOT برای بیان نقاط قوت، ضعف، فرصت‌ها و تهدیدات CEW در میدان نبرد استفاده شده است.

جدول (۶): تجزیه و تحلیل SWOT مفهوم CEW.

| نقاط قوت | نقاط ضعف |
|---|---|
| ➢ بسیار سریع زیرا از طیف EM استفاده می‌کند<br>➢ موجود در هزینه‌های کم<br>➢ قابل استقرار در سیستم عامل‌های مختلف با توجه به سطح اثر مورد نظر<br>➢ تحت تاثیر شرایط آب و هوایی قرار نمی‌گیرد | ➢ به اطلاعات عمیق و بیش‌تری نیاز دارد<br>➢ نیاز به غلبه بر برخی موانع برای نفوذ به سیستم‌های دشمن |

| | |
|---|---|
| ➢ تولید آسان، نیازی به کارخانه‌های جامع ندارد<br>➢ تشخیص سخت است. | ➢ به گیرنده‌های قدرتمندی برای تشخیص نقاط ضعف سیستم دشمن نیاز دارد |
| **فرصت ها** | **تهدیدها** |
| ۱. اثرات مطلوب زمانی به دست می‌آید که کنترل سیستم هدف قرار گیرد<br>۲. غیرکشندگی را فراهم می‌کند<br>۳. معیار CDC کم است<br>۴. می‌تواند بازدارنده باشد<br>۵. منطق سیستم هدف را می‌توان فریب داد<br>۶. شبکه‌های بسته را در معرض تهدیدات سایبری قرار می‌دهد<br>۷. نیروهای هوایی را برای استفاده مؤثر در عملیات سایبری فراهم می‌کند. نیروی هوایی می‌تواند در عملیات سایبری به طور مؤثر diyelim استفاده شود.<br>۸. حمله استراتژیک علیه مرکز ثقل دشمن را بهبود می‌بخشد<br>۹. می‌تواند به دفاع سایبری دشمن حمله کند<br>۱۰. مقابله با حملات سایبری را فراهم می‌کند<br>۱۱. می‌تواند با حمله معمولی به طور هم‌زمان اعمال شود<br>۱۲. اقتصاد نیرو را فراهم می‌کند | ۱. می‌تواند در برابر فریب آسیب‌پذیر باشد<br>۲. ارزیابی خسارت سخت است |
| **خلاصه تحلیل SWOT** | |
| در نتیجه تجزیه و تحلیل، نیروهای هوایی می‌توانند و ممکن است به طور مؤثر در CW مورد استفاده قرار گیرند. با توجه به حملات سایبری علیه سیستم‌های کنترل‌شده رایانه‌ای و روش‌های حمله الکترونیک سایبری برای سیستم‌های دفاع هوایی، نیروی هوایی می‌تواند بیشتر در معرض تهدیدات سایبری قرار گیرد، بنابراین، مهارت‌های حمله سایبری باید به شدت بهبود یابد. به‌علاوه، تحت تأثیر قرار دادن سیستم‌های رایانه‌ای که نمی‌توانند شبکه‌های بهره‌برداری را تحت تأثیر قرار دهند، توسط CEW می‌تواند آسان باشد. از طرفی، چون CDC آن کم است، استفاده از سیستم‌های حمله الکترونیکی سایبری می‌تواند رشد کند. | |

**۶- نتیجه‌گیری**

در این تحقیق، بر اهمیت فضای سایبری در منطقه رزمی تأکید شده است. روش‌های حمله سایبری با توجه به پیشرفت‌های فناوری اخیر در دو گروه حملات نرم‌افزاری و سخت‌افزاری مورد بررسی قرار می‌گیرند. نوآوری در فناوری، مفاهیم عملیات را تغییر داده و CEW به عنوان یک مفهوم جدید نظامی ظاهر شده است. استفاده یکپارچه از CW و EW می‌تواند از ابتدای جنگ به مناطق عملیاتی گسترده‌ای برسد. ضرورت وجود سلاح سایبری امری اجتناب‌ناپذیر شده است و برای رفع این ضرورت مطالعات خاصی انجام شده و برخی هنوز در حال انجام است. سیستم‌های حمله CEW می‌توانند بر سیستم‌های کامپیوتری و شبکه‌های ارتباطی در میدان نبرد تأثیر بگذارند. سیستم‌های بسته دشمن را می‌توان با تزریق نرم‌افزار مناسبی که در سیگنال‌های هدایت شده به آنها تعبیه شده است، به سیستم‌های باز تبدیل کرد. اگرچه استفاده از مفهوم CEW در یک حمله از نظر فناوری امکان‌پذیر است، امّا موانعی مانند پیچیدگی سیستم تهدید، نیاز به هوشمندی، انواع مختلف فایروال‌ها و رمزهای عبور وجود دارد. مفهوم CEW از نظر استفاده از نیروی هوایی در عملیات سایبری نقش مهمی دارد. با توجه به حل

مشکلات فوق، مفهوم CEW با استفاده از C4ISR، جنگ الکترونیک و جنگ سایبری در میدان نبرد، باعث پیشرفت‌های زیادی می‌شود.

**منابع:**


[1] Cavelty, M. D., "Cyber-Allies," Strengths and Weaknesses of NATO's Cyberdefense Posture. IP Journal, 2011. https://ip-journal.dgap.org/en/ip-journal/topics/cyber-allies.

[2] All About Stuxnet, 2010, Retrieved on 2010-11-06. http://www.stuxnet.net/

[3] Rash, W., "Lockheed Martin Network Attack Highlights Dangers of 'Cyber-Cold War'," Lockheed-Martin Network Attack Highlights Dangers of CyberCold War-190580/, 2011. http://www.eweek.com/c/a/Security/

[4] Electronic Warfare, Joint Publication 3-13.1., 2007.

[5] Cay, O., "Bilgi Harbi ve Turkiye (Information Warfare and Turkey)," 2009. http://savunmahaber.wordpress.com/

[6] Fahrenkrug, D. T., "Cyberspace Defined," National Military Strategy for Cyberspace Operations, 2007. http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm

[7] Cyberspace, Air Force Doctrine Document 2-11, United States Air Force, 2008.

[8] Koprulu, T., "Ag Destekli Yetenek Kapsamında Siber Savas Konsepti (Scope of Network Enabled Capability Concept Cyber War)," Ankara, 2010.

[9] Cyber Operations and Cyber Terrorism, DCSINT Handbook No. 1.02, 2005.

[10] Cifci, H., "Bilgi Harbinden Siber Savaslara Dogru (From Information Warfare to Cyber Warfares)", Ankara, Unpublished, 2012.

[11] Alford, L.D., "Cyber Warfare: To Threat to Weapon Systems," Cyber Warfare: Understanding The Threat To Weapon Systems, WSTIAC (Weapon Systems Technology Information Analysis Center), Quarterly Vol. 9, No. 4, 2009. http://wstiac.alionscience.com/quarterly

[12] Keggler, J. and Mahon, T., "Preparing for Cybergeddon," Armada International, April-May, 2009, http://findarticles.com/p/articles/mi_hb3031/is_2_33/ai_n31641640/

[13] Johnson, N. B., "Report: Cyber Attacks Targeted U.S. Satellites," Defense News, 2011. http://www.defensenews.com/article/20111028/DEFSECT01/110280301/Report-Cyber-Attacks-Targeted-U-S-Satellites

[14] Fulghum, D., "Army Embraces Airborne Electronic and Cyber-warfare," Aviation Week and Space Technology, 2010.

[15] Armed Forces Int. Technology Analyst, "Raytheon's Next Generation Jammer Power System Passes Technology Readiness Tests," 2010. http://www.armedforces-int.com/news-releases/raytheon-s-next-generation-jammer-power-system-passes-technology-readiness-tests.html

[16] Fulghum, D. , Dornheim, M. A. and Scott, W. B., "Black Surprises," Aviation Week and Space Tech.