

C4I یا جنگ اطلاعات

محمد مسبوق

چکیده:

پیروزی در نبردهای امروزه که در آنها تجهیزات بسیار پیشرفته با تاکتیک های پیچیده ای به خدمت گرفته می شود، از یک سو به اطلاعات به هنگام و قابل دسترس، و از سوی دیگر به تصمیم گیری سریع و منطقی نیاز دارد. انبوه اطلاعات تکنیکی و تاکتیکی و تغییر مداوم وضعیت صحنه نبرد، فرماندهان را ناگزیر به استفاده از ابزارها و روش هایی برای دستیابی بهینه از اطلاعات مورد نیاز نموده است. به طبع حجم عظیم اطلاعات دیگر مجال برای فرماندهان فراهم نمی آورد تا به صورت سنتی اطلاعات را با وسایل ابتدایی طبقه بندی و نگهداری نمایند. امروزه سامانه های C4I در کنار فرماندهان، اطلاعات لحظه ای مورد نیاز آنان را جمع آوری، پردازش و تجزیه و تحلیل می کنند، تا فرماندهان در اجرای تصمیمات خود با شجاعت دستورات را به یگان های زیر مجموعه جهت اجرای ماموریت واگذاری، بی درنگ صادر نمایند. در این میان، شناخت توانمندی دشمن و میزان دسترس وی به بهره برداری از امواج الکترومغناطیس سرگردان در فضای صحنه عملیات و حفاظت سامانه های C4I خودی در مقابل انواع تهدیدهای موجود در منطقه نبرد، فرماندهان را مجبور می سازد تا انواع ترفندهای مناسب را برای حفاظت از دسترسی و استراق سمع دشمن به سامانه های C4I بکار گیرند تا هم دشمن را ناامید و مایوس از بهره برداری اطلاعات خودی نمایند و هم توانمندی اطلاعات خود را در مقابل دشمن افزون سازد و این امری ضروری و اجتناب ناپذیر است:

کلید واژه: رایانه، سامانه، C4I، دفاع، اطلاعات، تهدید

مقدمه:

واژه C4I^۱، یا جنگ اطلاعات عبارت است از مجموعه تصمیم گیری‌های و اقدامات لازم و به موقع در جهت برتری اطلاعات بر دشمن که شامل اقداماتی نظیر ایجاد اختلال و از بین بردن سامانه‌های اطلاعاتی دشمن و نیز حفاظت از سامانه‌های اطلاعاتی خودی در مقابل نفوذ دشمن می‌باشد. تاریخ بشر از ابتدا تا به امروز همواره با جنگ و ستیز همراه بوده و خواهد بود. هدی و الوین تافلر^۲ در کتاب "جنگ و ضد جنگ" تاریخچه جنگ را با تکیه بر سه موج تقسیم نموده‌اند:

موج اول- موج کشاورزی^۳ است

موج دوم- موج صنعتی^۴ است

موج سوم- موج اطلاعات^۵ است

در خلال موج اول، تاکید جنگ بر خیل انبوه نیروهای انسانی و سربازان بود. در موج دوم یا موج صنعتی عاملی تعیین کننده برتری در جنگ، استفاده از سلاح کشتار جمعی و سامانه‌های مخابراتی و اداری بود و سعی فرماندهان برتری و تفوق در زمینه شنود مخابراتی و به طور کلی استفاده موثر از سامانه‌های C3I^۱ بوده است. در این نوع جنگ به علت استفاده از سلاح کشتار جمعی تلفات نیروی انسانی فوق‌العاده زیاد بود (جنگ جهانی دوم با کشته شدن ده میلیون از افراد بشر نمونه بارز آن بود).

1- Command, Control, Communication, Computer and Intelligence
2 - Hedi and Alvin Toffler
3 - Agrarian Wave
4 - Industrial Wave
5 - Information Wave

در جریان موج سوم، که موج اطلاعات نام گرفته است، ماهیت جنگ به شکل جنگ اطلاعات تغییر پیدا نموده است و برتری اطلاعات نقشی حیاتی ایفا می کند. لذا هدف اصلی فرماندهان و طراحان نظامی و دست‌اندرکاران در این نوع جنگ، برتری در زمینه فرماندهی و کنترل مبتنی بر سامانه‌های اطلاعاتی و شبکه‌های مخابراتی و رایانه‌های مرتبط با آن می‌باشد. که اصطلاحاً به آن C₄I می‌گویند.

حفاظت C₄I یا جنگ اطلاعات:

در عصر اطلاعات، حمله به سامانه‌های اطلاعاتی امری گریز ناپذیر است و به همین دلیل، دفاع در برابر حملات اطلاعاتی اهمیت قابل ملاحظه‌ای پیدا می‌کند. البته باید توجه داشت که دفاع کامل در مقابل حملات اطلاعاتی امری ایده‌آل و غیر واقع‌گرایانه است. لیکن، می‌توان در این زمینه تدابیری اتخاذ کرد که نتایج قابل قبولی در پی داشته باشد. منظور از دفاع در C₄I ممانعت از حملات اطلاعاتی، بی‌اثر کردن آنها و کنترل خسارات برجای مانده ناشی از آنها می‌باشد. برخی از تحلیل‌گران نظامی، جنگ خلیج فارس (۱۹۹۱) را، اولین جنگ اطلاعات و برخی دیگر آن را آخرین جنگ عصر صنعتی نامیده‌اند. در این جنگ، اطلاعات و استفاده از سامانه‌های C₄I قدرت و اهمیت خود را در مقابل درگیری سنتی و اتکا به سلاح متعارف و سامانه‌های C₃I به نمایش گذاشت. جنگ اطلاعات با حملات غیر فیزیکی به سامانه‌های اطلاعاتی و ادوات الکترونیکی دشمن آغاز می‌شود که نتیجه آن از بین بردن اطلاعات حیاتی دشمن، ایجاد اختلال در فرایندهای اطلاعاتی و تزلزل فرماندهان در تصمیم‌گیری بموقع می‌باشد.

جنگ اطلاعات دارای ویژگی‌هایی نظیر، دقت همراه با هزینه پایین، ریسک پذیری کمتر، گسترش حاشیه امنیت نیروهای خودی، اصل غافلگیری و غیره است که اهمیت آن را برای طراحان و دست‌اندرکاران نظامی برجسته می‌نماید. در این نوع جنگ، حریم امنیتی وجود ندارد. به عبارتی خط مقدم مفهوم خود را از دست می‌دهد. اکثر سامانه‌ها و شبکه‌های رایانه‌ای، مخابراتی، و شبکه‌های رادیو و تلویزیون، بخصوص شبکه فرماندهی و کنترل به نفع دشمن و بر علیه نیروهای خودی عمل می‌کنند. لذا پیش‌بینی می‌گردد که وقوع چنین جنگی، در جامعه‌ای که مورد هجوم قرار می‌گیرد، آسیب‌های اجتماعی، عدم اعتماد به نفس و فقدان کنترل را به دنبال داشته باشد. بدین ترتیب تأثیرات منفی اجتماعی آن می‌تواند خیلی بیشتر از خسارات واقعی پدید آمده باشد، همچنین رابطه غیر منطقی بین خسارات واقعی و آسیب‌های اجتماعی، مساله جنگ اطلاعات را به یک چالش ویژه تبدیل می‌کند.

موضوع مهم این است که در مقابل حملات اطلاعاتی نیروهای متعارف نظامی برای مقابل با آن کارآمد نیستند. به همین دلیل نکات و مسایل ویژه‌ای را باید مورد توجه قرار داد که در زیر به برخی از آنها به صورت اجمال اشاره می‌شود:

اولاً، مساله این نیست که یک حمله می‌تواند یا نمی‌تواند یک سامانه خاص را نابود یا مختل سازد، بلکه هدف خساراتی است که موجب دلهره و اضطراب همگانی می‌گردد.

ثانیاً سامانه‌های موجود بدون توجه به امور امنیتی و تا اندازه‌ای با سهل‌انگاری طراحی و ساخته شده‌اند. به عنوان نمونه می‌توان به اضطراب و نگرانی جهانی ناشی از مشکل سال ۲۰۰۰ سامانه‌ها و شبکه‌های رایانه‌ای و اطلاعات اشاره نمود. در نتیجه محافظت و ایمن کردن سامانه‌ها مشکل بوده و مستلزم توجه و تعمق زیادی می‌باشد.

ثالثاً، افزایش نیاز به ارتباطات آشنایی جوامع با فرهنگ نوین اطلاع‌رسانی و مزایای شبکه‌های جهانی نظیر اینترنت، موجب گسترش تعامل سامانه‌ها شده است. به صورت روشن، ضریب ایمنی این سامانه‌ها نیز به موازات گسترش خطوط آنها کاهش پیدا کرده است. از طرف دیگر فقدان متقابل تعامل، باعث انجام کارهای موازی، اتلاف منابع و کندی کار می‌گردد. بنابر این با ملحوظ داشتن ملاحظات امنیتی و فرهنگی باید از فرصت‌های ناشی از فناوری اطلاعات بهره‌برداری زیادی به عمل آورد. برای دفاع مناسب در جنگ اطلاعات و اتخاذ استراتژی دفاعی بهینه، شناخت انواع تهدیدها، اهمیت زیادی دارد، چرا که با توجه به نوع تهدید یا تهدیدها و تجزیه و تحلیل آنها، می‌توان استراتژی‌های مناسب را اتخاذ کرد.

دامنه تهدیدها را می‌توان در سه ناحیه مورد توجه قرار داد:

- ۱- ناحیه تهدیدهای روزمره
- ۲- ناحیه تهدیدهای استراتژیک
- ۳- ناحیه تهدیدهای استراتژیک بالقوه

تهدیدهای روزمره به توده وسیعی از تهدیدها اطلاق می‌شود که به طور مرتب و روزمره رخ می‌دهد و از لحاظ امنیتی اهمیت چندانی ندارند.

تهدیدهای استراتژیک بخش کوچکی از تهدیدها هستند که از لحاظ امنیتی قابل تامل و بررسی می‌باشند. **تهدیدهای استراتژیک بالقوه** از لحاظ امنیتی مشکل‌زا هستند و با توجه به این که بالقوه استراتژیک می‌باشند، چالشی سخت و قابل تعمق به حساب می‌آیند که می‌توان به صورت زیر به اهم آنها اشاره نمود.

۱- تهدید بر علیه سامانه‌های ایمنی و کنترل سلاح کشتار جمعی
۲- تهدید بر علیه حداقل تجهیزات ضروری شبکه‌های ارتباطی و مخابراتی

۳- تهدید بر علیه سامانه‌های ارتباطی و اطلاعاتی مربوط به سامانه فرماندهی و کنترل

شناخت تهدیدات در حفاظت C₄I از اهمیت بالایی برخوردار است. تناسب تهدید در هر منطقه‌ای به طور مستقیم بر روی ساختار نیروهای مسلح و در نتیجه بر شرایط C₄I تاثیر می‌گذارد. تهدیدها متناسب با شرایط دشمن در ابعاد نبرد، تجهیزات و ضرورت‌های ژئوپلیتیک منطقه قابل ارزیابی است. از طرفی نوع سامانه‌های به کار گرفته شده توسط دشمن و میزان کارایی آنها به عنوان پارامتر مهمی در تهدیدات نقش دارد. شرایط تهدیدات درون مرزی و برون مرزی در صحنه عملیات، ناشی از توان رزمی دشمن، نیروهای به کار گرفته شده، تکنیک‌ها و استراتژی‌های مربوطه بر ساختار سامانه‌های دفاعی C₄I تاثیر گذار هستند. در حال حاضر موثرترین سامانه دفاعی در

مقابل سامانه C₄I بهر گیری از توانایی‌های جنگ الکترونیک^۱ (EW) می‌باشد. امروزه فرماندهان رده تاکتیکی کاربرد جنگ الکترونیک را در تدبیر عملیاتی خود همانند یگان‌های توپخانه بخشی از توان رزمی خود مورد توجه قرار می‌دهند. جنگ الکترونیک، پشتیبانی اطلاعات عملیات رزمی و سایر عملیات غیر جنگی را فراهم کرده و یگان‌های اطلاعات نظامی، فرماندهان رده تاکتیکی و عملیاتی را در انواع عملیات رزمی پشتیبانی می‌نماید.

جنگ الکترونیک به طور کلی در سه بخش، تک الکترونیک^۲ (EA)، پشتیبانی جنگ الکترونیک^۳ (ES) و حفاظت الکترونیک^۴ (EP) عمل می‌کند.

در تک الکترونیک انرژی الکترومغناطیسی را برای ایجاد اختلال، خسارات، انهدام و کشتار نیروهای دشمن، به دو صورت انرژی کشنده (انرژی مستقیم) و غیر کشنده (پارازیت رسانی)^۵ به کار می‌برند.

در پشتیبانی جنگ الکترونیک اطلاعات لازم را توسط جداسازی، موقعیت یابی و بهره برداری از ارتباطات دشمن (بی سیم‌ها) و فرستنده‌های غیر ارتباطی (رادارها) جمع آوری می‌نماید، و اطلاعات به موقع را که مورد نیاز فوری تصمیم‌گیری فرماندهی است، ارائه می‌دهد. اطلاعات بدست آمده از این طریق (ES)، تمام منابع تجزیه و تحلیل، تک الکترونیک، حفاظت الکترونیک را پشتیبانی می‌نماید و به عنوان یک منبع اطلاعاتی

-
- 1 - Electronic Warfare
 - 2 - Electronic Attack
 - 3 - Electronic Warfare Support
 - 4 - Electronic Protection
 - 5 - Jamming

روی نیازهای فوری فرماندهان در زمینه نیات دشمن و کسب اطلاعات از هدف گیری دشمن تمرکز می نماید.

جنگ الکترونیک قادر است سامانه های الکترونیکی، کارکنان و تجهیزات خودی را از اثرات نامطلوبی که توانایی های ارتباطی آنان را کاهش داده یا منهدم می کند، محافظت نماید؛ پس از پایان عملیات توفان صحرا در منطقه خلیج فارس (۱۹۹۱) صاحب نظران نظامی اظهار نظر نمودند که:

" برنده جنگ بعدی، کشوری خواهد بود که بهترین بهره برداری را از طیف امواج الکترونیک بنماید "

نیروهای ایالات متحده امریکا عملیات توفان صحرا را با اعتماد کامل به برتری الکترونیکی اجرا نمودند. ماهواره های مستقر بر فراز منطقه (قلمرو فضایی عراق) ارتباطات عراقی ها را شناسایی کرده و با انجام جنگ الکترونیک، صدام و عوامل اطلاعاتی او را کر و کور نمودند، به طوری که قطع صدور فرمان از بغداد، موجب عدم تحرک، عکس العمل کم، دریافت و دسترسی به کمترین اطلاعات، حداقل توانایی در هماهنگی و عدم تعامل بین عناصر زمینی، هوایی و دریایی نیروهای عراقی شد. به عبارت ساده تر، سامانه C₃I عراق بدون حفاظت به طور کلی مختل گردید. این امر در راستای فناوری اطلاعات و کارآمدی سلاح هوشمند، کاهش تلفات نیروهای خودی و نفوذ و اختلال در سامانه های اطلاعاتی طرف مقابل را بوجود آورد. مقابله با کارایی و نفوذ انواع ویروس های رایانه ای در سامانه C₄I، ساختار سامانه توسط افراد مجاز و مورد اطمینان، تصدیق هویت، صدور مجوز دستیابی، ممانعت از انکار عمل، حسابرسی و ثبت وقایع،

دیواره‌های آتش، مکانیزم‌های رمز نگاری و در نهایت کاربرد بهینه از جنگ الکترونیک به صورت صحیح، همه و همه نقش حیاتی و حساسی را در برابر حفاظت C₄I به عهده دارند.

نتیجه:

انواع فناوری‌های پیش رو، عصر جدیدی را در توسعه فنی و تجهیزاتی سامانه‌های C₄I ایجاد نموده است. نگاه مداوم به این فناوری‌های نو و پیشرفته به منظور حفظ و تقویت توان رزمی نیروها برای دستیابی به یک سامانه C₄I اثر بخش برای نیروهای مسلح لازم و ضروری است. تمایل روز افزون دشمن برای نفوذ و کسب خبر از خطوط مخابراتی و سامانه‌های C₄I به منظور بهره برداری، لزوم شناخت دامنه تهدیدها و اتخاذ تدابیر لازم در همه زمینه‌ها، از جلوگیری امکان شکستن سامانه‌های رمز نگاری گرفته تا توانمندی انواع نرم افزارها در مقابل کارایی تنوع ویروس‌های رایانه‌ای و کارآمدی جنگ الکترونیک در حفاظت از C₄I، می‌تواند توان تسلیحاتی نیروهای مسلح را در مقابل حفاظت سامانه‌های C₄I افزایش دهد. چرا که بدون تکیه به یک سامانه C₄I که دارای سرعت و دقت و اثر بخشی مناسبی باشد، برای هر ارتشی در عملیات غیر ممکن است. شناخت توانمندی دشمن در آسیب رسانی به این سامانه‌ها و عملیات خنثی سازی آنها از اهم دغدغه‌های فرماندهان در صحنه نبرد امروزی است.

منابع:

- 1- <http://www.disa.mil/08/html>
- 2- <http://www.sees.gwu.edu/~reto/infowar/example.htm>
- 3- <http://www.sees.gwu.edu/~reto/infowar/history.htm>
- 4- <http://www.prb.cam.com/C4I.htm>