فصلنامه
پژوهشی
آموزشی
علوم
و فنون
نظامی

سال دوم
شماره۳

حفاظت C_4I یا جنگ اطلاعات

محمد مسبوق

چکیده:

پیروزی در نبردهای امروزه که در آنها تجهیزات بسیار پیشرفته بـا تاکتیـک هـای پیچیده‌ای به خدمت گرفته می‌شود، از یک سو به اطلاعات به هنگام و قابـل دسـترس، و از سوی دیگر به تصمیم گیری سـریع و منطقـی نیـاز دارد. انبـوه اطلاعـات تکنیکـی و تاکتیکی و تغییر مداوم وضعیت صحنه نبرد، فرماندهان را ناگزیر به اسـتفاده از ابزارهـا و روش‌هایی برای دستیابی بهینه از اطلاعات مورد نیاز نموده است. بـه طبـع حجـم عظـیم اطلاعات دیگر مجالی برای فرماندهان فراهم نمی‌آورد تا به صورت سنتی اطلاعات را با وسایل ابتدایی طبقه بندی و نگهداری نمایند. امروزه سامانه‌های C_4I در کنار فرماندهان، اطلاعات لحظه‌ای مورد نیاز آنان را جمع آوری، پردازش و تجزیه و تحلیل می‌کننـد، تـا فرماندهان در اجرای تصمیمات خود با شجاعت دستورات را به یگان‌های زیر مجموعـه 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 سامانه‌های C_4I خودی در مقابل انواع تهدیدهـای موجـود در منطقه نبرد، فرماندهان را مجبور می‌سازد تا انواع ترفندهای مناسب را بـرای حفاظـت از دسترسی و استراق سمع دشمن به سامانه‌های C_4I بکار گیرند تا هم دشـمن را ناامیـد 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، C_4I ، دفاع، اطلاعات، تهدید

مقدمه:

واژه C_4I[1]، یـا جنـگ اطلاعـات عبـارت اسـت از مجموعـه تصـمیم 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 دشـمن و نیز حفاظت از سامانه‌های اطلاعاتی خودی در مقابل نفوذ دشمن می‌باشـد. تاریخ بشر از ابتدا تا به امروز همواره با جنگ و ستیز همـراه بـوده و خواهـد بود. هدی و الوین تافلر[2] در کتاب " جنگ و ضد جنگ" تاریخچه جنگ را با تکیه بر سه موج تقسیم نموده‌اند:

موج اول- موج کشاورزی[3] است

موج دوم- موج صنعتی[4] است

موج سوم- موج اطلاعات[5] است

در خلال موج اول، تاکید جنگ بر خیل انبوه نیروهای انسانی و سـربازان بود. در موج دوم یـا مـوج صـنعتی عـاملی تعیـین کننـده برتـری در جنـگ، استفاده از سلاح کشتار جمعی و سامانه‌های مخـابراتی و اداری بـود و سـعی فرماندهان برتری و تفوق در زمینه شنود مخـابراتی و بـه طـور کلـی اسـتفاده موثر از سامانه‌های C_3I بوده است. در این نـوع جنـگ بـه علـت اسـتفاده از سلاح کشتار جمعی تلفات نیروی انسانی فوق‌العاده زیاد بود (جنـگ جهـانی 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 می‌کند. 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 C_4I می‌گویند.

حفاظت C_4I 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 اطلاعات امری ایده‌آل و غیر واقع گرایانه است. لیکن، می‌توان در این زمینه تدابیری اتخاذ کرد که نتایج قابل قبولی در پی داشته باشد. منظور از دفاع در C_4I ممانعت از حملات اطلاعاتی، بی اثر کردن آنها و کنترل خسارات برجای مانده ناشی از آنها می‌باشد. برخی از تحلیل گران 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 C_4I قدرت و اهمیت خود را در مقابل درگیری سنتی و اتکا به سلاح متعارف و سامانه‌های C_3I 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 تصمیم گیری 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 پیش بینی 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 تاثیرات 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 سهل انگاری 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 اطلاع رسانی 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 می گردد. بنابر این با ملحوظ داشتن ملاحظات امنیتی و فرهنگی باید از فرصت‌های ناشی از فناوری اطلاعات بهره برداری 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 C_4I از اهمیت بالایی برخوردار است. تناسب تهدید در هر منطقه‌ای به طور مستقیم بر روی ساختار نیروهای مسلح و در نتیجه بر شرایط C_4I تاثیر می‌گذارد. تهدیدها متناسب با شرایط دشمن در ابعاد نبرد، تجهیزات و ضرورت‌های ژئوپلتیک 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 C_4I تاثیر گذار هستند. در حال حاضر موثرترین سامانه دفاعی در

مقابل سامانه C_4I بهر گیری از توانایی‌های جنگ الکترونیک[1] (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[2] (EA)، پشتیبانی جنگ الکترونیک[3] (ES) و حفاظت الکترونیکی[4] (EP) عمل می‌کند.

در تک الکترونیکی انرژی الکترومغناطیسی را برای ایجاد اختلال، خسارات، انهدام و کشتار نیروهای دشمن، به دو صورت انرژی کشنده (انرژی مستقیم) و غیر کشنده (پارازیت رسانی[5]) به کار می‌برند.

در پشتیبانی جنگ الکترونیکی 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 تصمیم گیری فرماندهی است، ارائه می‌دهد. اطلاعات بدست آمده از این طریق (ES)، تمام منابع تجزیه و تحلیل، تک الکترونیکی، حفاظت الکترونیکی 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 می‌نماید.

جنگ الکترونیک قادر است سامانه‌های الکترونیکی، کارکنان و تجهیزات خودی را از اثرات نامطلوبی که توانایی‌های 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. ماهواره‌های مستقر بر فراز منطقه (قلمرو فضایی عراق) ارتباطات عراقی‌ها 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، عکس‌العمل 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 ساده‌تر، سامانه C_3I 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 سامانه‌های اطلاعاتی طرف مقابل را بوجود آورد. مقابله با کارایی و نفوذ انواع ویروس‌های رایانه‌ای در سامانه C_4I ، 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 C_4I به عهده دارند.

نتیجه:

انواع فناوری‌های پیش رو، عصر جدیدی را در توسعه فنی و تجهیزاتی سامانه‌های C_4I ایجاد نموده است. نگاه مداوم به این فناوری‌های نو و پیشرفته به منظور حفظ و تقویت توان رزمی نیروها برای دستیابی به یک سامانه C_4I اثر بخش برای نیروهای مسلح لازم و ضروری است. تمایل روز افزون دشمن برای نفوذ و کسب خبر از خطوط مخابراتی و سامانه‌های C_4I 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 C_4I ، می‌تواند توان تسلیحاتی نیروهای مسلح را در مقابل حفاظت سامانه‌های C_4I افزایش دهد. چرا که بدون تکیه به یک سامانه C_4I 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

۵- تافلر، هدی و الوین، جنگ و ضد جنگ، ترجمه بشارت دوست، مهدی، انتشارات امیرکبیر، تهران، ۱۳۷۷