چالش های کاربردی و توسعگی جنگ اطلاعاتی در کشور

سید ضیاءالدین قاضی زاده فرد[1]

چکیده :

در دنیای پر تلاطم امروزجهت دستیابی به امنیت پایدار، برخورداری از راهبرد مناسب برای ایجاد نظم و تأمین امنیت و ثبات در جوامع و بهره گیری مناسب از فناوری های نوین اطلاعاتی، بسیار مهم است. دولتمردان از یک سوی و نیروهای مسلح کشورها از سوی دیگر، باید درکنار راهبردهای نظامی برای شکست دشمن، ویژگی های فناوری اطلاعاتی و جنگ های مجازی و اطلاعاتی را مورد توجه ویژه قرار دهند، زیرا امروزه این دو مکمل یکدیگر محسوب می گردند.

در جهان امروز که شاهد ستیزها ومنازعات متعدد، در تمامی سطوح و در بین کشورها بوده و ماهیت جنگ ها در عصر اطلاعات، دچار تغییر و تحول اساسی گردیده اند، نیاز به آسیب شناسی و به کارگیری شیوه ها و راهبردهای نوین و مناسب برای تعامل و تقابل با جنگ های اطلاعاتی از ضروریات است.

در این مقاله با ارایه تعاریفی از جنگ های اطلاعاتی، ویژگی ها و ابعاد آنها را توضیح داده و انواع روش ها در این نوع جنگ ها معرفی شده است و در انتها پیشنهادهایی برای اجرا در نیروهای مسلح ارائه گردیده است.

واژه های کلیدی: فناوری اطلاعات، جنگ اطلاعاتی، ویژگی های جنگ های اطلاعاتی، لشکرها و تیپ های اطلاعاتی

۱ - استادیار و عضو هیئت علمی دانشگاه امام حسین(علیه السلام)

مقدمه

در سال های گذشته،گفته می شد: زمانی خواهد رسید که سرعت رخ دادن وقایع، ماورای مدیریت انسان قرار می گیرد. این زمان اکنون فرا رسیده است.یکی از جاهایی که در آن حجم انبوه اطلاعات، انسان های با ظرفیت روحی و جسمی محدود را مغلوب می سازد، اتاق وضعیت عملیات (اتاق جنگ) است. در یک عملیات نظامی، فرمانده ممکن است هر لحظه با پدیده انفجار اطلاعاتی روبرو شود. اطلاعات مربوط به جو و زمین، ترکیب، آمادگی و گسترش نیروهای خودی و دشمن و گزارش های متنوعی که هر لحظه از مسیر ها و واسطه های مختلف انسانی و ماشینی به او می رسد، لحظه ای او را آرام نمی گذارد. از طرفی اطلاعات رسیده ازدرجه‌های ارزشی متفاوتی برخوردارند. گاهی اطلاعات یک لشکر از اطلاعات یک دسته رزمی که در موقعیت زمانی و مکانی خاصی قرار گرفته است، اهمیت کمتری دارد. برخی اطلاعات باید به تناوب زمانی ساعتی، روزانه و هفتگی به فرمانده برسد و برخی لحظه ای. فرمانده باید در اتاق وضعیت خود، در زمان واحد این اطلاعات غیر همگون را بشنود و ببیند، اطلاعات بی اهمیت را جدا سازد و اطلاعات با اهمیت را در ذهن خود تجزیه و تحلیل نماید تا براساس آنها برای فرماندهان زیر دست خود دستور صادر کند، به هم رده ها اطلاع دهد و به فرماندهان بالاتر خود گزارش کند وهرلحظه ، چگونگی اجرای فرمان های خود را کنترل نماید و ... پس از آن، باز هم اطلاعات جدیدتری از راه می رسد و باز هم به همین ترتیب پردازش آن اطلاعات صورت می‌پذیرد[سعیدی کیا، 1380]

بیان مسأله

با پیشرفت سرسام آور فناوری،هر لحظه بر تعداد، تنوع و کیفیت این اطلاعات افزوده می شود. همان گونه که روشن است سیستم های سنتی جمع آوری، پیش پردازش، پردازش و نمایش اطلاعات جوابگو نخواهند بود. برای این که فرماندهان با انبوهی از اطلاعات نامنظم مواجه نشوند و بتوانند در سطح بالاتر فرماندهی و کنترل به طور موفق عمل کنند، باید به نوعی به سیستم های رایانه ای متصل باشند که خاصیت پردازش انبوه داده ها را با سرعت و دقت بالا داشته باشند. به همین دلیل نیز در جنگ های مهمی چون جنگ خلیج فارس، رایانه‌ها بیشترین نقش را در فرماندهی و کنترل ایفا می کردند. در این زمینه گفته شده است که: جنگ

خلیج فارس جنگی بود که در آن یک اونس سیلیکون در یک رایانه، بیش از یک تن اورانیوم ارزش داشت.

پیشرفت رایانه ها و نقش آفرینی آنها در نبردهای امروزی تا آنجا پیش رفته که بسیاری از نظریه پردازان نظامی به اغراق گفته اند: روزی فراخواهد رسید که بیشتر سربازان به جای تفنگ، رایانه به دست گیرند و البته دیده می شود که در بسیاری از سلاح های پیشرفته انفرادی، این پردازنده ها و تجهیزات رایانه‌ای اسلحه هستند که مرکز ثقل سلاح محسوب می شوند، نه سیستم های شلیک آن. بنابراین در دنیای امروز، ارتش‌های مدرن، حل بسیاری از مشکلات انسانی فرماندهی و کنترل را به ماشین های دقیق و هوشمندی به نام رایانه سپرده اند و به صورت لحظه ای می توانند اطلاعات را در چرخه مناسب و مورد نظرشان به گردش درآورند و از آنها استفاده نمایند.

فرماندهی که تسلط و احاطه کاملی بر وضعیت های پیش آمده نداشته باشد، اطلاعات مؤثر دریافت نکند یا در انبوهی از اطلاعات غرق شود و توانایی جداسازی اطلاعات مهم را از انبوه اطلاعات کم اهمیت تر و هم چنین قدرت ارتباط سریع را با فرماندهان بالاتر، هم تراز و زیر دست خود نداشته باشد، حتی اگر به کوله‌باری از تجربه و اعتقاد و کوهی از سلاح های ویرانگر مجهز باشد، ضعیف و شکننده خواهد بود.

ضرورت واهمیت تحقیق

در یک نبرد تاکتیکی (وحتی راهبردی)، سه عامل مهم و سرنوشت ساز عبارتند از: جوّ، زمین، نیروهای خودی و نیروهای دشمن. هر سه این عوامل به نوعی در تغییر مداوم وضعیت نقش دارند. نیروهای خودی و دشمن هر لحظه در حال اجرای دستورها و انجام عملیات می‌باشند و با هر حرکت و شلیک و تغییر در اندازه، ظرفیت و ترکیب این نیروها، وضعیت جدیدی به وجود می آید.

فرمانده باید هر لحظه از این تغییر وضعیت ها مطلع شود تا بتواند بر مبنای آن تصمیم گیری کند. بنابراین در یک جنگ اطلاعاتی، چرخه مداومی از جریان اطلاعات وجود دارد. اطلاعات وضعیت منطقه نبرد پس از جمع آوری، پردازش می شود و فرمانده بر اساس آنها

تصمیم می گیرد. دستور فرمانده به یگان های زیردست ابلاغ می شود و با انجام عملیات توسط آنها،وضعیت دیگری به وجود می آید و... این چرخه تکرارمی شود.

درسال های پایانی قرن بیستم، انقلاب عظیمی در زندگی بشرتحت تأثیر انفجار بزرگی به نام انفجار اطلاعات[۱]، تحت عنوان انقلاب اطلاعاتی[۲] به وقوع پیوسته است و رشد فناوری اطلاعات و تحولات حاکم بر آن، بر عرصه های مختلف زندگی انسان ها و جوامع تأثیر به سزایی گذاشته و اقتصاد، صنعت، فرهنگ، کشاورزی، خدمات و بخش های عظیمی از جوامع گوناگون را تحت تأثیرات چشمگیری قرار داده است و این روند در سال‌های اولیه قرن بیست و یکم با سرعت شگفت آوری در حال پیشرفت است.

ادبیات تحقیق

درجامعه الکترونیکی[۳] که در سطح جهان رو به فزونی و گسترش است، دولت ها همپای سازمانهای الکترونیکی دربخش خصوصی، خدمات خود را درقالب دولت الکترونیکی[۴] به شهروندان الکترونیکی[۵] خود ارائه می‌نمایند، نیروهای مسلح درمرزهای کشور با دیده بانی الکترونیکی[۶] از امنیت کشور پاسداری نموده و با دفاع الکترونیکی[۷]، حریم کشور را از تعرض بیگانگان حفظ می نمایند و جنگ‌های خود را نیز در قالب جنگ الکترونیک[۸] و تمرینات نظامی خود را نیز با بهره گیری از انواع شبیه سازها (سیمیلاتورها) و نرم افزارهای مربوط به بازی جنگ[۹] و برگزاری رزمایش‌الکترونیکی[۱۰]،توسط لشکرهای اطلاعاتی انجام داده و انواع مهمات خود را به شکل مهمات اطلاعاتی[۱۲] در آورده و آنها را نیز در زاغه های اطلاعاتی[۱۳] نگهداری می نمایند.

۱ - Information Explotion
۲ - Information Revolution
۳ - E-Society
۴ - E-Government
۵ - E- Citizen
۶ - E- Look Out
۷ - E-Defence
۸ - E-Warfare
۹ - War Game
۱۰ - E-Maneouvre
۱۱ - Information Army
۱۲ - Information Armament
۱۳ - Information Depot

هدف تحقیق

بدیهی است که در این شرایط جهانی، سازمان های نظامی کشور ما نیز دستخوش تحولات گوناگونی شده و آنها نیز درموقعیت ها و شرایطی غیر از وضعیت گذشته قرار گرفته‌اند و این شرایط جدید نیز هم فرصت‌ها و هم تهدیدات و چالش هایی را برای آنها در پی خواهد داشت که شناخت آن برای فرماندهان، مدیران و کارکنان نیروهای مسلح امری ضروری می‌باشد.

تحت این شرایط، ادبیات سازمان های نظامی وجنگ ها، به دلیل پیدایش و توسعه فناوری اطلاعات در سطح و عمق آنها دچار تغییر و تحولات اساسی شده و بسیاری از مفاهیم و اصطلاحات گذشته و فنون فرماندهی و سازماندهی درجنگ ها و عملیات های رزمی، تغییر یافته و تحت تأثیر این مفاهیم جدید قرار گرفته اند.

آنچه که فناوری اطلاعات برای فرماندهان، مدیران و کارشناسان و رزمندگان عرصهٔ نبردها به ارمغان می آورد، قدرت بی سابقهٔ پردازش اطلاعات دیجیتالی به مدد سیستم های اطلاعاتی رایانه ای است که تلفیقی از سخت افزارها، نرم افزارها ، شبکه ها، داده ها و انسانها هستند.

مفاهیم تحقیق

مفاهیمی چون ارتش الکترونیکی[۱]،دفاع الکترونیکی، تک (تهاجم) الکترونیکی[۲]، حفاظت الکترونیکی، برتری اطلاعاتی[۳]، حفاظت و امنیت اطلاعات[۴]و ... همه و همه در انقلاب اطلاعاتی که در دنیای سازمان های نظامی نیز رخ داده است، معنا و مفهومی جدید را پیش روی نظریه‌پردازان نبردهای سنتی قرارداده است.

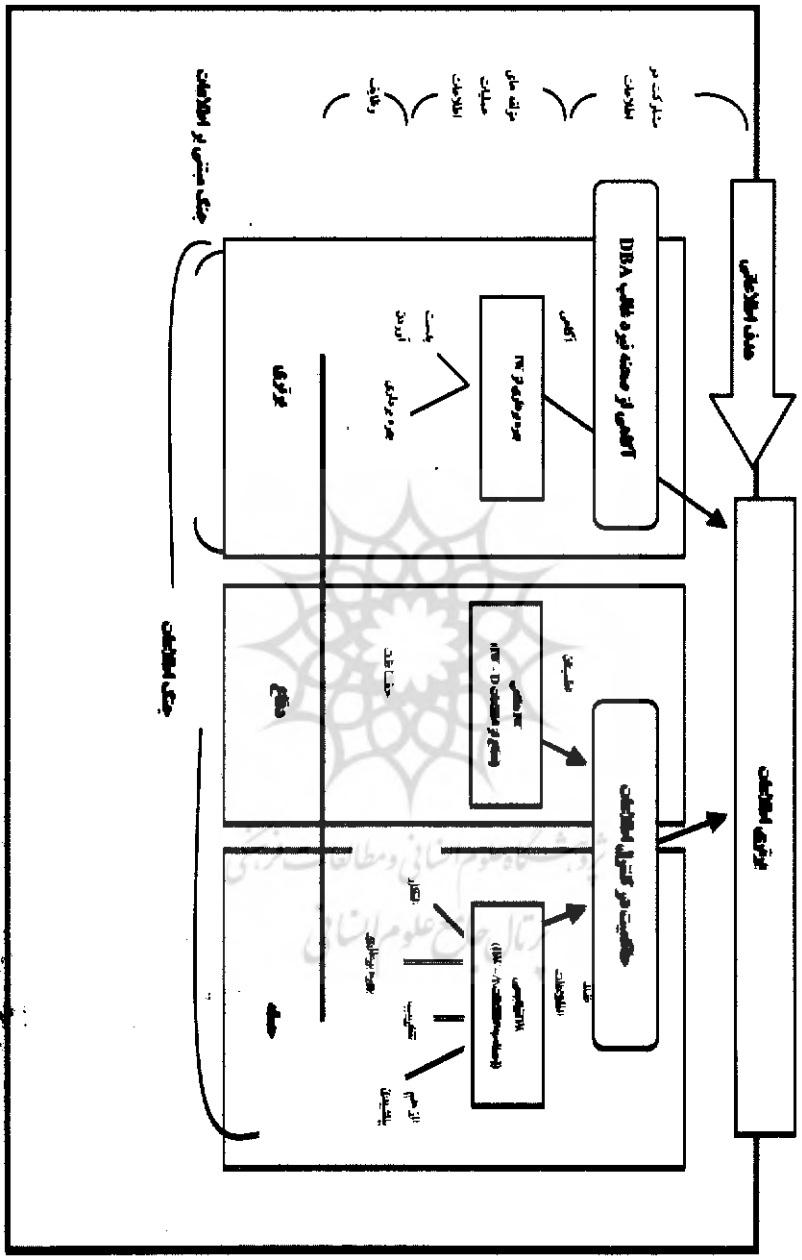
این انقلاب اطلاعاتی، ابزارها و روش های جدیدی را در اختیار نیروهای مسلح کشورهای مختلف قرار داده تا با بهره گیری از آنها از سرمایه های ملی و مردم کشور خود دفاع نمایند. حتی ممکن است برای برخی از کشورها مقابله با قدرت های بزرگ نظامی از طریق فناوری های متعارف درجنگ های هسته ای، شیمیایی، میکروبی و سلاح های پیشرفته کشتار جمعی

۱- E - Army
۲- E -Attack
۳- Information Superiority
۴- E - Security

موشکی، هوایی، دریایی و زمینی امکان پذیر نباشد ولی ممکن است رویارویی و مقابله به مثل در میدان و عرصه جنگ اطلاعاتی ،همان گونه که مؤلفه ها و اهداف عملیات در جنگ های اطلاعاتی در شکل شماره (۱) ارائه گردیده است، به عنوان عرصه ای جدید مقدور باشد.

کشورهای توسعه یافته به دلیل برخورداری از ساختارهای اجتماعی باز و زیرساخت ها و بزرگراه‌های اطلاعاتی[1] و مخابراتی گسترده، در مقابل جنگ های اطلاعاتی بسیار آسیب پذیرتر خواهند بود. شاید درعمل نیز اتکای این کشورها به نبردهای اطلاعاتی ، غیرعملی و غیرمنطقی باشد، چرا که هنگامی که جنگ های اطلاعاتی با ویژگی‌هایی همچون سرعت عمل، هزینه های ناچیز ، اثر بخشی و کارآیی، با ابزار و تجهیزات قابل دسترس، عدم نیاز به کشتار و خون ریزی گسترده ، افزایش قدرت بازدارندگی و امکان حضورگسترده مردم در نبردهای اطلاعاتی و... درمقابل دولتمردان، برنامه ریزان و فرماندهان و کارشناسان نظامی دیگر کشورها وجود دارد تمایل و پرداختن آنها به جنگ های سنتی با ابزارها وتجهیزات گران قیمت و پرهزینه و دریسیاری از موارد دست نیافتنی، کمتر خواهد شد واین ها می تواند رویکرد ابرقدرت ها رادرمخاصمات بین‌المللی تغییر اساسی بدهد.

[1] - Information Highway



شکل شماره (۱)– مؤلفه ها و اصناف عملیات در جنگ های اطلاعاتی

خلاصه آنکه رایانه ها و سیستم های اطلاعاتی مبتنی بر آنها، لشکری ازسربازان سریع، دقیق، خستگی ناپذیر، ارزان، بی باک، شجاع و حرف شنو هستند که می توانند فرماندهان خود را از دغدغهٔ عملیات گسترده و حجیم و پرهزینه با پردازش پرحجم و سنگین اطلاعات فارغ نموده و توانایی ها و قابلیت های آنها را به سطوح بالاتری از فرماندهی ارتقا دهند.

بنابراین استفاده از فناوری اطلاعات نه تنها به عنوان یک ابزار، بلکه به عنوان یک راهبرد جدید و حیاتی جهت حفظ برتری اطلاعاتی بر دشمن در جنگ های آتی که از ویژگی جنگ اطلاعاتی برخوردار هستند، مورد توجه فرماندهان و کارشناسان نیروهای مسلح کشورها قرار گرفته و درحال حاضر بسیاری از کشورها مبادرت به تدارک زیرساخت های لازم برای حداکثر بهره برداری از این فناوری، برای مقابله با دشمنان در نبردهای آتی احتمالی، نموده‌اند و در سازمان خود پیش بینی های لازم را تدارک دیده اند [احمدی مهربانی، ۱۳۸۰].

قدرت نظامی به « قابلیت های کنونی و آینده یا توان نیروهای مسلح یک کشور یا چند کشور متحد در مقایسه با قابلیت های کنونی و آینده دشمنان حال و آینده آنها» اطلاق می گردد [حقیری و ستاری خواه، ۱۳۸۴: ۱۶۵].

در تعریف زیرساخت های حیاتی هم باید عنوان نمود که زیرساخت به طور کلی مجموعه ای از عناصر ساختاری به هم پیوسته ای هستند که چارچوبی را برای پشتیبانی کردن از یک ساختار کلی ایجاد می کند. بنابراین زیرساخت های حیاتی یک کشور شامل زیرساخت‌های سرمایه ای، تأسیسات و تجهیزات، ساختمان ها، عوامل انسانی در زیرساخت های تبادل اطلاعات می گردند [عبدا.. خانی، ۱۳۸۴: ۱۹۲ - ۱۹۰].

جنگ در مقابل حل و فصل مسائل به روش مذاکره و دیپلماتیک، شدیدترین نوع برخورد انسان ها تلقی می گردد. دو طرف درگیری در جنگ تمامی سعی و تلاش خود را در جهت نابودی طرف مقابل به کار می گیرند تا به پیروزی دست یابند و جنگ اطلاعاتی روشی برای اجرای این اهداف می باشد. [والتز[1]، ۱۳۸۵: ۳]

[1] - Edward Waltz

عبارت جنگ اطلاعاتی برای اولین بار حدود سی سال قبل یعنی در سال ۱۹۷۶ توسط فردی به «نام توماس رونا[1]» که یکی از صاحب نظران حوزه جنگ‌های اطلاعاتی محسوب می گردد، به کار گرفته شد و به ویژه طی دو دهۀ اخیر به عنوان مفهوم جدیدی در ادبیات نظامی و مراکز راهبردی نظامی مشاهده می‌شود. به گونه ای که پیش بینی می شود یکی از اهداف مهم در منازعات و جنگ های آینده، سیستم های اطلاعاتی طرف های متخاصم باشد. به همین دلیل برتری نیروهای مسلح کشورها در آشنایی و تسلط به شیوه های مختلف جنگ‌های اطلاعاتی ، به عنوان یک برگ برنده در منازعات میان کشورها محسوب می گردد[رونا، ۱۹۹۶: ۱۳۲].

برای جنگ اطلاعاتی تعاریف مختلف و متفاوتی ارائه شده است که در زیر به چند نمونه آنها اشاره می‌شود:

(۱) مجموعه تصمیم گیری ها و اقدامات لازم و به موقع در جهت برتری اطلاعات بر دشمن که شامل اقداماتی نظیر ایجاد اختلال و ازبین بردن سامانه های اطلاعاتی دشمن و نیز حفاظت از سامانه های اطلاعاتی خودی در مقابل نفوذ دشمن می باشد [امیر صوفی، ۱۳۷۹].

(۲) به کلیۀ اقداماتی اطلاق می شود که از طریق اثرگذاری بر اطلاعات و سیستم های اطلاعاتی دشمن و به منظور دستیابی به برتری اطلاعاتی، در راستای راهبرد نظامی یک کشور صورت پذیرد [طرح فرا سازمانی فاوا، ۱۳۸۵].

(۳) جنگ اطلاعات شامل اقدامات لازم جهت حفظ یکپارچگی سامانه های اطلاعاتی خودی در مقابل بهره برداری،آلوده شدن وتخریب و از طرف دیگر تلاش برای بهره برداری ،آلوده کردن و تخریب سامانه های اطلاعاتی دشمن و انجام پردازش های لازم جهت به دست آوردن برتری اطلاعاتی در مواقع اعمال فشار می باشد[والتز، ۱۳۸۵: ۲۶].

بررسی تاریخی تحقیق

در آغاز سال ۲۰۰۰ به دلیل تبدیل عدد ۹۹ به ۰۰ در رایانه ها، بسیاری از سیستم‌های رایانه‌ای دچار مشکلات عدیده ای شدند و میلیاردها دلار هزینه شد تا این مشکل مرتفع و سامانه‌های عملیاتی از کار نیفتند. این پدیده نشان داد که از جنگ اطلاعاتی می توان به عنوان

[1] - Thomas P. Rona

ابزاری قوی برای از کار انداختن سیستم های اطلاعات طرف متخاصم استفاده مناسب نمود.

حادثه یازده سپتامبر در آمریکا نیز بیش از هرچیز دیگری، نارسایی سیستم امنیتی آن کشور در برابر حملات تروریستی را به اثبات رساند. اگرچه آمریکا در دهه پس از پایان جنگ سرد توانسته بود بزرگ ترین زرادخانه نظامی تاریخ بشر را تدارک ببیند ؛ به نحوی که هیچ کشوری در جهان جرأت حمله نظامی به آن کشور را نداشته و ندارد؛ اما حمله غیرمتعارف یازده سپتامبر، این معادله را برهم زد و مقامات عالی رتبه امنیتی آمریکا ناگهان با این حقیقت مواجه شدند که امنیت داخلی این کشور در برابر حملات تروریستی و غیرمتعارف بسیار آسیب پذیر است. آنها بر این اعتقاد بودند که تروریست ها توانسته اند از آزادی های فردی و اجتماعی داخل آمریکا و همچنین نظارت محدود اف. بی. آی و با کمک گرفتن از خلاء های امنیتی و عدم نظارت کافی بر حوزه های ارتباطی و اطلاعاتی، ضربه هولناکی را به امنیت داخلی آمریکا وارد کنند. بنابراین نخستین پیامد حملات تروریستی مزبور، تلاش برای تقویت امنیت داخلی و به ویژه ارتقای توانمندی امنیتی در حوزه های اطلاعات بود. زیرا با توجه به حوادث و روند موجود در داخل آمریکا از سال ۲۰۰۱ به بعد و با عنایت به این که فناوری های ارتباطاتی و الکترونیکی نقش مهمی در جامعه آمریکا دارند، این نگرانی در ذهن متولیان حوزه امنیت پدید آمد که در صورت حملات رایانه ای به بخش های مالی، حمل و نقل، مخابرات و امثال آن چه باید کرد؟وچگونه می توان از سوء استفاده اطلاعاتی خرابکاران جلوگیری کرد؟ در این راستا و برای جلوگیری ازتشدید نگرانی های داخلی چهاراقدام صورت گرفت [عباسی اشلقی،۱۳۸۵: ۱۸۳]:

۱) تلاش گردید ظرفیت های وسیع نظارتی و مراقبتی توسعه پیدا کند و هماهنگی بیشتری در بخش های مختلف برای جمع آوری و تحلیل اطلاعات پدید آید.

۲) تلاش شد تا با کمک وسایل ارتباطی از شدت تهدیدهای فزاینده که ذهنیت روانی جامعه را مغشوش کرده بود، کاسته شود.

۳) کوشش هایی در جهت ایجاد شرایط مناسب اجتماعی در جهت مقابله و جنگ با تروریسم انجام شد.

۴) تلاش هایی در جهت تقویت امنیت اطلاعاتی، ارتباطی و الکترونیکی به ویژه در حوزه‌های ارتباطات ، حمل و نقل و مالی صورت گرفت.

تا پیش از این تنها سازمان سیا متولی اصلی حوزه امنیت و محور اقدامات محسوب می شد ولی از سال ۲۰۰۱ به بعد چند تحول در این عرصه پدید آمد، که مهم ترین آنها تشکیل وزارت امنیت داخلی بود که با دستور رئیس جمهور آمریکا و تصویب کنگره در خرداد ۱۳۸۱ (ژوئن۲۰۰۲) تأسیس شد. اهداف اصلی این وزارت نیز در چهار بخش؛ امنیت مردمی و سیستم حمل و نقل، مقابله با حملات شیمیایی، میکروبی و رادیولوژیک، آمادگی برای اقدامات اضطراری و تجزیه و تحلیل اطلاعات و حفاظت زیربنایی، تعریف شد. در این زمینه باید توجه داشت، از آنجا که سیستم های مختلف اجتماعی درون آمریکا از ارتباطات الکترونیکی و اطلاعاتی پیچیده‌ای سود می برند هرگونه اخلال درآنها بزرگ ترین نارسایی را درنظام اجتماعی آمریکا پدید می آورد، بنابراین مهم ترین وظیفه این وزارت، حفاظت از زیرساخت های حیاتی نظیر حمل و نقل، اطلاعات و ارتباطات مخابراتی، نظام مالی و بانکی، صنایع دفاعی و پست، کشتیرانی و امثال آن است و مقرر گردید که از طریق ارتباط مؤثر با سازمان های مربوط، تحلیل سازواره همه اطلاعات برای پیشگیری از وقوع خطرات صورت گیرد.

تهدیدات جدید در حوزه های امنیت داخلی آمریکا و دیگر کشورهای غربی در عصر اطلاعات موجب شده است که مقامات امنیتی این کشورها در تصور تهدیدات داخلی خود تجدیدنظر کرده و تلاش نمایند تا به ارتقای امنیت در شبکه ها و سیستم های اطلاعاتی و حوزه های نرم افزاری خود بپردازند.

«هیدی و الوین تافلر»در کتاب جنگ و ضد جنگ تاریخچه جنگ ها را در طول قرون و اعصار گذشته به سه موج تقسیم و تشبیه نموده اند[بشارت، ۱۳۷۴] :

موج اول: موج کشاورزی

موج دوم: موج صنعتی

موج سوم: موج اطلاعات

در جریان موج اول تأکید جنگ برخیل انبوه نیروهای انسانی و سربازان بود. در موج دوم یا موج صنعتی، عامل تعیین کننده برتری در جنگ، استفاده از سلاح های کشتار جمعی و

سامانه های مخابراتی و راداری بود و به طور کلی استفاده مؤثر از سامانه های (C_3I)[1] بود. در این نوع جنگ به علت استفاده از سلاح‌های کشتار جمعی تلفات نیروی انسانی فوق العاده زیاد بود. به عنوان مثال جنگ دوم جهانی باکشته شدن بیش از ده میلیون انسان ازافراد بشرهمراه بود.

در جریان موج سوم که موج اطلاعات نام گرفت، ماهیت جنگ ها به شکل جنگ اطلاعات تغییر پیدا نموده است و برتری اطلاعاتی نقش حیاتی را ایفا می کند. بنابراین هدف اصلی فرماندهان و طراحان نظامی دست اندرکار این نوع جنگ ها، برتری در زمینه فرماندهی و کنترل مبتنی بر سامانه های اطلاعاتی و شبکه های مخابراتی و رایانه ای مرتبط با آن می باشد که به آن (C_4I) گفته می شود[امیر صوفی، ۱۳۷۹].

(C_4I) به معنای فرماندهی، کنترل، ارتباطات، رایانه و خبرگیری است و امروزه یکی از موضوعات تحقیقاتی و کاربردی در اکثر ارتش های جهان می باشد. شاید در یک تعریف اجتمالی بتوان گفت:

(C_4I) مجموعه ای از سخت افزارها، نرم افزارها، روش ها و افرادی است که در مدیریت اطلاعات نظامی نقش دارند [نقش بندی، ۱۳۷۹].

قبل از تعریف جنگ اطلاعات لازم است اهداف جنگ ها بیان شود. هدف بشر در جنگ ها از بین بردن تجهیزات ، تأسیسات، نیروها، توانمندی ها و استعدادهای نظامی و غیرنظامی و اقتصادی طرف مقابل (دشمن) است، به گونه‌ای که منجر به تسلیم یا ترک مخاصمه یا تسلط بر آن شود.

با توجه به این تعریف بیشتر دولت مردان قدرت نظامی را پیش نیازی برای بقای ملی قلمداد می کنند. قدرت نظامی: «مجموع قدرت نیروهای مسلح یک کشور به همراه دیگر عناصر قدرت ملی که شامل قدرت سیاسی، قدرت اقتصادی، قدرت اجتماعی ـ فرهنگی و توانایی زمامداران کشور در به کارگیری این نیروها جهت پشتیبانی از سیاست های ملی می باشد».[حقیری و ستاریخواه، ۱۳۸۴: ۱۶۵].

«سان تی زو[2] »کارشناس نظامی چینی در قرن ششم قبل از میلاد در کتاب هنر جنگ گفته است: در شرایط عملی جنگ، بهترین کار ، تصرف کامل سرزمین دشمن، بدون دست

[1] - Command, Control, Communication & Intelligence

خوردگی می باشد. بنابراین جنگیدن و پیروزی در جبهه های جنگ، امتیازی محسوب نمی‌شود، درمقابل موفقیت درگروشکست مقاومت دشمن بدون جنگیدن است [والتز، ۱۳۸۵: ۵].

هریک از این تعاریف بیان کنندهٔ دیدگاه ویژه ای در مورد رویارویی اطلاعاتی می‌باشند، اما به نظر نگارنده تعریف زیر می تواند تعریفی جامع و کامل ازجنگ اطلاعاتی باشد:

«به مجموعه ای از اقدامات و عملیات نظامی و غیرنظامی که با بهره گیری از کلیه توانمندی‌های اطلاعاتی، سیستمی، تجهیزاتی و انسانی اعم از نظامی و غیر نظامی یک کشور،امکان برتری اطلاعاتی را از طریق شنیدن، دیدن و درک بهتر از اطلاعات مربوط به سیستم ها و استعدادها و توانمندی‌های دشمن، فراهم آورده و با انجام خرابکاری و ایجاد هرج و مرج و اختلال در آنها و با حفظ منابع و سیستم های اطلاعات خودی، امکان دستیابی به اهداف سیاسی، اقتصادی، اجتماعی یا نظامی را برای یک کشور فراهم آورد، جنگ اطلاعاتی اطلاق می شود»[قاضی زاده، ۱۳۸۵].

در کتاب پر تیراژ جنگ سایبرنتیکی می آید توسط «جان آرکیولا[1]» و «دیوید رون فلد[2]» از نویسندگان «راند[3]»چهار نوع جنگ اطلاعاتی، همان گونه که در جدول شماره (۲) نشان داده شده، بر مبنای گسترش و توسعه زیر ساخت های اطلاعاتی مشخص گردیده است. در جدول مزبور انواع جنگ ها به ترتیب نزولی براساس سطح درگیری ایدئولوژیکی قرار گرفته اند[والتز، ۱۳۸۵: ۲۱].

[1] - Arquilla
[2] -David Ronfeldt
[3] - Rand

جدول شماره (۲)- مقایسه شکل های مختلف جنگ اطلاعات از نظر آرکیولا و رون فلد

شکل جنگ	اهداف [1]	روش ها	مورد هدف [2]
جنگ شبکه ای	مدیریت بر برداشت‌های جوامع مورد هدف جهت ایجاد تأثیر دلخواه بر رفتار ملی	مدیریت بر برداشت ها از طریق مخابرات شبکه و کنترل اطلاعات به منظور تأثیر همه جانبه بر هدف های اجتماعی	کل جامعه (به لحاظ سیاسی، اقتصادی و نظامی)
جنگ سیاسی	تأثیر گذاری بر تصمیمات و سیاست‌های رهبران دولت ها	به روش تأثیر گذاری بر سامانه سیاسی کشور و سازمان های دولتی	سامانه های سیاسی
جنگ اقتصادی	تأثیر گذاری بر تصمیمات و سیاست‌های رهبران دولت ها	به روش تأثیرگذاری بر اقتصاد کشور از طریق تولید و توزیع محصولات (تحریم، بلوکه کردن و دزدی فناوری)	سامانه های اقتصادی
C2W (جنگ سایبرنتیک)		عملیات نظامی علیه اصول اطلاعاتی شامل بهره برداری از دانش، جنگ روانی، فریب و جنگ الکترونیک می شود.	سامانه های نظامی

[1] - Objective
[2] - Targets

انواع روش ها در جنگ های اطلاعاتی

در دهۀ اخیر، جنگ اطلاعاتی موجب تحول در محیط منازعات بین المللی شده است. در این راستا حملات از دو طریق یکی با حملات عینی نظیر بمباران نظامی یا انهدام تأسیسات نظامی و غیرنظامی و دیگری از طریق حملات مجازی نظیر تخریب زیرساخت های اطلاعاتی و ارتباطی، قطع خطوط ارتباطی و صدمه زدن به بخش های الکترونیکی قابلیت اجرا پیدا کرده‌اند. برای مقابله با حملات نوع دوم که در حال افزایش نیز می باشند، نیاز است تا از تاکتیک و نحوۀ عمل مشخصی بهره گرفت.

در راستای عوامل یاد شده، تهدید و هجوم به ساختارهای اطلاعاتی به سه روش به گونه ای که در جدول شماره (۳) معرفی گردیده امکان پذیر است[عباسی اشلقی، ۱۳۸۵: ۱۸۰]:

هدف فنی	هدف حمله	محور امنیت اطلاعات
سرقت یا استفاده غیرقانونی از اطلاعات ارزشمند	سوء استفاده از سیستم های اطلاعاتی رقیب	نخست: محرمانه بودن
منحرف کردن یا تغییر دادن اطلاعات رقیب یا سیستم های اطلاعاتی	پخش و توزیع اطلاعات غلط یا گمراه کننده	دوم: انسجام و یکپارچگی
تخریب اطلاعات مهم و کلیدی، فلج کردن سیستم های اطلاعاتی دشمن	تخریب نمودن یا از کار انداختن سیستم های اطلاعاتی دشمن	سوم: دستیابی

جدول شماره (۳)- روش های تهدید و هجوم به ساختارهای اطلاعاتی

در سطح نخست تلاش می شود تا به اطلاعات محرمانه و ارزشمند رقیب دسترسی پیدا کنند و از این طریق ضربه خویش را وارد نمایند. در سطح دوم از طریق توزیع و پخش اطلاعات گمراه کننده و غلط تلاش می شود تا یکپارچگی و انسجام ملی تضعیف گردد و در

سطح سوم برای تخریب سیستم های اطلاعاتی رقیب و از کار انداختن آنها تلاش می شود. جهت مقابله و دفاع در برابر تهاجم اطلاعاتی باید در درجه اول انواع جنگ های اطلاعاتی و مقاصد آنها را شناخت و مطالعه نمود و در درجه دوم متناسب با هرکدام از روش ها، تاکتیک های مناسب را اتخاذ کرد.

گسترش فناوری اطلاعات دو پیامد مشخص بر اوضاع اجتماعی و دموکراسی خواهد داشت. نخست این که چگونگی ساختار قدرت و پاسخ گویی در رأس یک نظام سیاسی تحت تأثیر قرار خواهد گرفت و دوم اینکه چگونگی روابط متقابل مردم و دولت، دگرگون خواهد شد. در عصر اطلاعات مردم به راحتی از چگونگی و کیفیت تصمیم ها و نحوهٔ اجرای آنها مطلع می شوند و دولت نیز موظف به پاسخگویی در برابر اقدامات صورت گرفته خواهد بود. به سختی می توان مردم را در یک خلاء اطلاعاتی قرار داد و امور سیاسی و اجتماعی را مخفیانه و به تدریج پیش برد. در این خصوص سه مشکل اساسی برای حکومت ها قابل تصور است. نخست پیامدهای جنگ اطلاعاتی بر اتخاذ و اجرای تصمیمات در هنگام جنگ، دوم تأثیر اطلاعات تحریف شده در قضاوت های نادرست افکار عمومی درباره رهبران و دولتمردان، سوم امکان ایجاد لوازم و تجهیزات دفاعی در زمینه جنگ اطلاعاتی و سوق یافتن دولت به سمت دخالت بیش از اندازه در زندگی شهروندان.

باید توجه داشت که فناوری اطلاعات موجب ارتقای سطح آگاهی جامعه شده و دولت ها نمی توانند به راحتی و بدون اقناع افکار عمومی، اقدامات موردنظر خود را انجام دهند، استفاده از فناوری اطلاعات برای ارائه اطلاعات صحیح و صریح به جامعه و اداره امورسیاسی، فرهنگی، اجتماعی وامنیتی از جمله اقدامات ظریفی است که بایدموردتوجه قرارگیرد [اشلقی، ۱۳۸۵: ۱۸۰].

با توجه به گستردگی حضور اطلاعات و سیستم های اطلاعاتی درعرصه های مختلف زندگی بشر و در جوامع مختلف، در ادبیات منتشر شده در این حوزه، در تقسیم‌بندی به کارگیری روش های مختلف درجنگ‌های اطلاعاتی،کمتر اتفاق نظر بین پژوهشگران وجود دارد. مهمترین روش هایی که در بسیاری از آثار مربوط به صاحب نظران برجسته مشاهده می شود، عبارتند از :

(۱)جنگ فرماندهی وکنترل C4I

(۲)جنگ الکترونیک[1]

(۳)جنگ هوشمند مدار[2]

(۴)جنگ روانی[3]

(۵)جنگ نفوذگران (سارقان) رایانه ای[4]

(۶) جنگ اطلاعات اقتصادی[5]

(۷)جنگ اطلاعات رایانه ای در فضای مجازی[6]

(۸)جنگ اطلاعات راهبردی[7]

(۹)جنگ شبکه مدار[8] [روزنا، 1996] و [قاضی زاده، ۱۳۸۵] و [والتز، ۱۳۸۵: ۲۳] و [طرح فراسازمانی فاوا نیروهای مسلح، ۱۳۸۵: ۱۱۶]

ویژگی ها و ابعاد جنگ های اطلاعاتی

بسیاری بر این باورند که اگر تقابل و رویارویی با دشمن و قدرت های بزرگ نظامی دنیا با روش‌ها و تجهیزات و تسلیحات متعارف و معمول، امکان پذیر نباشد یا با کاستی هایی همراه باشد، ضربه زدن به دشمن از طریق جنگ های اطلاعاتی امکان پذیر می باشد . این امر امروزه به عنوان نقطه ضعف قدرت های بزرگ نظامی دنیا تلقی می‌گردد، چرا که اهداف غیرنظامی زیادی به غیر از اهداف نظامی، در معرض تهاجمات نیروی متخاصم قرار می گیرند.

ویژگی های جنگ های اطلاعاتی را می توان به صورت خلاصه و چکیده در هیجده محور به شرح زیر مطرح و معرفی نمود

(۱) حضور توده ای آحاد مردم به شکل سازمان یافته و سازمان نیافته (بسیج مردمی خودجوش)؛

[1] - Electronic Warfare
[2] - Intelligence – Based Warfare
[3] - Psychological Warfare
[4] - Hacker Warfare
[5] - Economic Information Warfare
[6] - Cyber Warfare
[7] - Strategic Information Warfare
[8] - Network Centric Warfare

(۲) پایه گذاری بر مبنای توسعه و استفاده از فناوری اطلاعات؛

(۳) امکان قطع ارتباطات شبکه های دسترسی داخلی، ملی و بین‌المللی؛

(۴) صرفه جویی در زمان جمع آوری، پردازش و انتقال اطلاعات و کاهش زمان اجرای عملیات؛

(۵) تبادل سریع اطلاعات وتسهیل در ارتباطات بین سطوح مختلف فرماندهان ورزمندگان؛

(۶) دسترسی سریع و آسان به اطلاعات صحیح، کامل، جامع، به هنگام، به موقع، موجز، دقیق، مناسب، مرتبط، کارآمد و اثر بخش؛

(۷) افزایش سرعت و دقت در تصمیم گیری توسط فرماندهان سطوح مختلف؛

(۸) افزایش سرعت جنگ ها و توسعه میدان نبرد و مناطق عملیاتی و درگیری؛

(۹) قابلیت دسترسی مناسب تر و ارزان تر به ابزار و امکانات و تسلیحات و تجهیزات نظامی؛

(۱۰) ایجاد هماهنگی مناسب تر بین یگان های آموزشی، آماد و پشتیبانی و عملیاتی؛

(۱۱) تسهیل آموزش های انسانی و افزایش بهره وری دوره های آموزشی؛

(۱۲) اجتناب از به کارگیری تسلیحات و تجهیزات گسترده به صورت غیر اثربخش و ناکارآمد؛

(۱۳) وارد آوردن ضربات مؤثر وکارا بردشمن و مهیا شدن زمینهٔ برتری اطلاعاتی و پیروزی کامل؛

(۱۴) جلوگیری ازافزایش تلفات انسانی دوطرف تخاصم به ویژه شهروندان ومردم عادی؛

(۱۵) کم هزینه بودن و داشتن صرفه اقتصادی؛

(۱۶) افزایش قدرت بازدارندگی کشورها؛

(۱۷) تشدید درگیری بین چند کشور با ظهور همکاری های مجازی؛

(۱۸) توسعه خلاقیت ها و ابتکارات فردی؛[قاضی زاده، ۱۳۸۶] و [کاستلز، ۱۳۸۰] و [نورمن[1]، 1996] ، [گلدمن[2]، 2004] و [مولاندر و دیگران[3]، 1996]

بررسی و داده پردازی

خاتمه دوران جنگ سرد و درس های ناشی از عملیاتی نظیر طوفان صحرا و حمله آمریکا به عراق و تحولاتی که منجر به ایجاد تغییر نظام جهانی شده اند، اصول و مبانی جدید رزمی را دیکته می کنند که نیازمند روش ها و فناوری جدیدی در زمینه حفظ امنیت ملی وجهانی است.

بنابراین باید ضمن استفاده از تجربیات نظامی گذشته، از فناوری آینده در حفظ کیفیت نیروهای رزمی بهره برد. سیستم های مبادله اطلاعات جهانی، سیستم های مبادله اطلاعات تاکتیکی، شبکه های داده های دفاعی، سیستم های جنگ الکترونیکی، جنگ نفوذگران (سارقان) رایانه ای، جنگ شبکه مدار، (C4I) و جنگ اطلاعاتی، نمونه هایی از نفوذ بلامنازع فناوری اطلاعات در سیستم های نظامی و فرماندهی و کنترل آن هستند.

پیشرفت رایانه ها و نقش آفرینی آنها در نبردهای امروزی تا آنجا پیش رفته است که بسیاری از نظریه پردازان نظامی به اغراق گفته اند: روزی فرا خواهد رسید که بیشتر سربازان به جای تفنگ، رایانه به دست گیرند.

در دوران قبل از پیروزی انقلاب اسلامی، ارتش ایران با پشتیبانی کامل به تجهیزات تاحدودی پیشرفته رایانه ای به ویژه در نیروی هوایی و وزارت جنگ مجهز شده بود و شرکت ایزایران برای پشتیبانی نرم افزاری و سخت افزاری تجهیزات مزبور ایجاد گردید.

دوران بعد از انقلاب را به دو دوره دفاع مقدس و دوره سازندگی می توان تقسیم نمود. در دوران دفاع مقدس، نیروهای مسلح با پشتیبانی همه سازمان های غیرنظامی در تلاش بودند که جلوی پیشرفت دشمن بعثی در خاک میهن عزیز را گرفته و در نهایت آنها را با خفت و خواری از مرزهای غربی و جنوبی کشور بیرون اندازند. تجربیات جنگ الکترونیک به صورت محدود با بهره گیری از تجهیزات پیشرفته ای که از خارج خریداری می گردید و یا به دست متخصصان پرتلاش ایرانی ساخته شده بود، انجام می پذیرفت.

[1] - Davis Norman
[2] - Emily Goldman
[3] - Molander & Riddile & Wilson

در دوران سازندگی این توجه به تجهیز نیروهای مسلح به تجهیزات مناسب برای جنگ الکترونیک ادامه یافت هر چند سرعت و شتاب این حرکت ها منطبق با سرعت و شتاب در حال انجام در کشورهای توسعه یافته که خود را برای جنگ های اطلاعاتی آماده و مجهز می کردند، نبود ولی موفقیت های فراوانی را تجربه نمود.

ولیکن چالش های اساسی که در دوران توسعه نیافتگی گرداگرد نیروهای مسلح با آن مواجه هستند عبارتند از:

(۱) نبود شناخت کامل و مناسب ابعاد مختلف سیستم های لازم برای جنگ های اطلاعاتی؛

(۲) عدم طراحی، توسعه و پیاده سازی کامل و مناسب سیستم های اطلاعاتی رایانه ای و شبکه های اطلاعاتی رایانه ای مناسب در سطح نیروهای مسلح و عدم توسعه و تقویت مناسب شرکت وابسته اند برای انجام پروژه های لازم در نیروهای مسلح.

(۳) نبود طرح جامع مناسب و کامل در نیروهای مسلح این کشور ها برای سیستم های لازم جهت جنگ های اطلاعاتی؛

(۴) نبود راهبرد و سیاست های کلان کامل و مناسب برای تجهیز نیروهای مسلح به ابزارها و تجهیزات مناسب برای جنگ های اطلاعاتی؛

(۵) نبود نظام تأمین نیروی انسانی مناسب و کامل برای جذب، آموزش، سازماندهی و به کارگیری نیروی انسانی ماهر و آماده برای شرکت در جنگ های اطلاعاتی در رده های مدیران و فرماندهان ارشد، میانی، عملیاتی و نیروهای رزمنده و عمل کننده؛

(۶) عدم توجه و عنایت کامل و مناسب به زیرساخت های لازم در مورد قوانین و مقررات، تحقیق و توسعه و سایر شرایط و ابزارهای لازم برای شرکت مؤثر در جنگ های اطلاعاتی؛

نتیجه گیری و پیشنهادها

(۱) درجنگ آتی دشمن قبل از آن که خود را درگیر جنگ نظامی نماید، سیستم‌های اطلاعاتی نظامی و غیرنظامی کشور مانند سیستم ها و شبکه های برق، مخابرات و تلفن، سوخت رسانی، مترو، سامانه های بانک ها، هواپیمایی، بندرگاه ها و ... و همه سیستم های

اجرایی و عملیاتی که مبتنی بر شبکه و رایانه باشند را مورد حمله اطلاعاتی قرار می دهد و تلاش خواهد کرد آنها را از پای درآورد. بنابراین تلاش در جهت ایمن کردن این سیستم ها و افزایش قدرت بازدارندگی و مقابله به مثل به همه دست اندرکاران و مسئولین نیروهای مسلح توصیه می گردد.

(۲) جنگ خلیج فارس و حمله آمریکا به عراق نمونه های جدیدی از جنگ اطلاعاتی مدرن بود، بررسی ابعاد مختلف مراحل این جنگ ها، نمایانگر این نکته است که تنها ارتش هایی در جنگ های آتی به پیروزی خواهند رسید که به وضوح جنگ اطلاعاتی را فراگیرند و به طور موفقیت آمیزی این جنگ را در زمین و هوا و دریا به مرحله عمل در آورند. بنابراین مرور کامل این نوع جنگ ها به ویژه دو جنگ اخیر برای آشنایی بیشتر با ابعاد جنگ اطلاعاتی توصیه می گردد.

در جنگ احتمالی آتی، دشمن به احتمال زیاد یگان ها و نیروها و ارتباطات خطوط مقدم کشور را با کاربرد سلاح، فنون و روش های جنگ اطلاعاتی فلج و زمین گیر خواهد کرد. دشمن تلاش خواهد کرد که رادیوها ، بی سیم ها، رادارها و سایرفرستنده های الکترونیکی نیروهای مسلح را با پارازیته کردن، عملیات فریب، تداخل و انهدام با آتش به کمک دستگاه‌های جهت یاب و موقعیت یاب از پای در آورد. یگان های مانوری نیروهای مسلح زمانی می‌توانند سرپا بمانند و در چنین میدان های رزمی بجنگند که در زمان صلح به طور کامل با فنون و تخصص ها و تجهیزات جنگ اطلاعاتی آشنا شوند و آموزش های لازم را دیده و آن را هنگام اجرای رزمایش ها تمرین کرده باشند. بنابراین پیشنهاد می گردد که در کلیه رزمایش های آتی، به کارگیری و اجرای جنگ اطلاعاتی در دستور کار فرماندهان عملیاتی حاضر در رزمایش ها باشد.

(۳) شناخت نوع تهدید برای هر کشوری ، ضرورت زیادی دارد. با توجه به این که اگر در آینده جنگی رخ دهد، آمریکا و متحدانش از جمله رژیم اشغالگر قدس (اسراییل) خطر عمده ای برای کشورهای مسلمان به خواهند بود، آگاهی از مقدورات این کشورها ضرورتی انکارناپذیر دارد. مسئولین دفاعی کشور و فرماندهان ارشد نیروهای مسلح باید به برتری

الکترونیکی و ارتباطی در جنگ اطلاعاتی که در حال حاضر در نیروهای مسلح این کشورها وجود دارد، عنایت ویژه داشته باشند و برای مقابله با آنها تدارک لازم را ببینند.

(۴) تا جایی که امکان پذیر است تمام سخت افزارها و نرم افزارهایی که طراحی شبکه ها و سیستم های اطلاعاتی و به ویژه آنهایی که در طراحی سیستم های مرتبط با جنگ های اطلاعاتی به کار برده می شوند، باید در داخل کشور ایجاد گردند تا هم حفاظت و امنیت سیستم ها تأمین و فراهم گردد و هم از توقف و ایستایی آنها توسط عملیات جاسوسی از سوی سازندگان یا فروشندگان آنها و یا در مواقع بحرانی و تحریم های نظامی و غیر نظامی جلوگیری به عمل آید.

(۵) با نظر اجمالی به نقش جنگ اطلاعات می توان نتیجه گرفت که در تمام جنگ‌های آتی، چه در مناطق خاکی و چه در مناطق آبی و چه در زمین و چه در هوا و فضا، اگر درگیری رخ دهد، در ابر متراکمی از امواج الکترومغناطیسی ناشی از وسایل ارتباطی و غیر ارتباطی و سیستم های جنگ الکترونیک صورت خواهد گرفت. بنابراین ضروری است که طراحان و فرماندهان نظامی و مسئولین امنیت ملی و دفاعی کشور توجه زیادی به جنگ اطلاعاتی و توانایی های کشور در این زمینه بنمایند.

اگرچه جنگ الکترونیک، در هیچ جنگی به تنهایی برنده جنگ نبوده و نخواهد بود اما غرب و تمامی کشورهای جهان متوجه شده اند که کنترل میدان رزم، یعنی کنترل طیف الکترومغناطیسی.

(۶) علاقه فرماندهان به ارزیابی کارایی سیستم ها و تجهیزات و سلاح های به کار رفته در عملیات، علاقه اپراتورها برای پی بردن به دقت هدف یابی و برد سلاح ها در زمان‌های مختلف شبانه روز، اشتیاق طراحان سیستم های تسلیحاتی برای ملاحظه حداکثر تخریب آنها روی منابع و ذخایر، و نیز علایق سایر متخصصین، کشور را به یک سیستم بسیار قوی فرماندهی، کنترل، ارتباطات، رایانه در جنگ‌های اطلاعاتی نیازمند می سازد. پس لازم است سیستم های مناسب برای جنگ های اطلاعاتی که با اهداف امنیت ملی هماهنگ و پاسخگوی نیازهای راهبردی، عملیاتی و تاکتیکی در وضعیت بحرانی باشد، ایجاد گردد.

(۷) برخلاف برخی تصورات ، به کارگیری، راه اندازی، بهره برداری و نگهداری انواع فناوری های نرم افزاری، سخت افزاری، شبکه ای، مخابراتی و الکترونیکی در صورت توان بومی سازی امن آن ، امری ضروری در نیروهای مسلح بوده و توسعه‌ی آنها نیز به یک عزم و برنامه جدی و بلندمدت ملی نیاز دارد تا در زمانی نه چندان کوتاه مدت و نه بلند مدت، دستیابی به این قابلیت ها در تمام سطوح نیروهای مسلح کشور مهیا گردد.

(۸) آموزش مدیران و فرماندهان عالی و ارشد و میانی نیروهای مسلح در اولویت اول و توسعه دانش و آگاهی و آموزش نیروهای شاغل در بدنه نیروهای مسلح و به ویژه فرماندهان یگان های عملیاتی و پرورش و توسعه نیروهای متخصص و متفکر، اولین اقدام در راستای این کار می باشد.

(۹) استفاده از فناوری اطلاعات در نبردها، زمینه برتری اطلاعاتی را در امر تصمیم‌گیری برای فرماندهان نیروهای مسلح فراهم می آورد. چرا که با الکترونیکی، دیجیتالی و رایانه ای کردن سیستم‌های رزمی اعم ازسیستم های آموزش، رزمایش، آماد و پشتیبانی، دیده بانی، اطلاعات شناسایی، رهگیری اهداف، انجام عملیات آتش در آفند و پدافند علیه دشمن و ... تبادل اطلاعات، به هنگام و آنی انجام می پذیرد. این امر موجب می گردد که زمینهٔ ایجاد تصویر و تصور یکسانی از وضعیت و شرایط نیروهای خودی و دشمن برای مدیران و فرماندهان میدان و فضای نبرد به وجود آید. بدیهی است اولین نتیجه این شرایط، کاهش درصد خطا ، خطرپذیری افزایش سرعت نبرد در بعد زمان و مکان و کاهش هزینه ها و صرفه جویی اقتصادی و بالا بردن سرعت واکنش ها به رخدادهای صحنه جنگ می باشد. اینها همه موجب افزایش توان رزم و مقابله با دشمن در نقاط مناسب و افزایش قدرت آفند و پدافند و قدرت انهدامی نیروها و در نهایت قدرت بازدارندگی گردیده و پیروزی قاطع و سریع را در مخاصمات به دنبال خواهد آورد.

با وجود تمام مزایا و محاسن و فرصت های ویژه ای که فناوری اطلاعات در توانمندی‌های نیروهای مسلح در نبردهای آتی به ارمغان می آورد، استفاده از آن در سازمان های نظامی مستلزم ایجاد بسترهای مناسب برای توسعه و افزایش ضریب نفوذ به کارگیری آن در سطح و عمق سازمان ها و بدنه نیروهای مسلح می باشد.

(۱۰) تقویت واحدها و ادارات ستادی با اختیارات ویژه و سطح بالا، برای برنامه ریزی، نظارت، کنترل و هدایت فرایند تحول فناوری اطلاعات درسطح نیروهای مسلح به ویژه در ستاد کل نیروهای مسلح برای هدایت بلند مدت این فرایند ضروری است.

(۱۱) لازم به تأکید است که در دنیای پرتنش عصر اطلاعات، که در حال گذار گریزناپذیر به سوی جامعهٔ اطلاعاتی و اطلاعات مدار می باشد، در روابط بین کشورها و دولت ها بهبود روابط و تقویت و توسعه و تحکیم روابط با ایجاد تعاملات سازنده درروابط امری ضروری و اجتناب ناپذیر می‌باشد. چه نیکوست که درکنار مدیران و فرماندهان نیروهای مسلح که درجهت دفاع از کشور، شرف و حیثیت ملی کشورها اقدام می نمایند، دولت ها با دولتمردان خود نیز در این راستا قدم های بلندتر و استوارتری را بردارند تا هیچ گاه در جهان شاهد نبرد و مخاصمه بین انسان ها و کشورها به ویژه از نوع جنگ های اطلاعاتی نباشیم.

در انتها تأکید می شود که تشکیل و راه اندازی لشکرها، تیپ ها و گردان های اطلاعاتیَ برای درگیر شدن در جنگ های اطلاعاتی به ویژه برای پدافند در مقابل آفندهای اطلاعاتی دشمن از امور بسیار واجب و ضروری در سطح نیروهای مسلح می باشد که می باید در کوتاه ترین زمان ممکن به ایجاد آنها اهتمام ورزید.

منابع ومآخذ

الف) فارسی

(۱)- احمدی مهربانی، محمد رضا (۱۳۸۰): «مدیریت اثربخش IT، ضرورت بقای سازمان در قرن بیست و یکم»، ماهنامه روش، ویژه نامه فناوری اطلاعات، تهران.

(۲)- امیر صوفی، رحمت ا... (۱۳۷۹): «اهمیت و نقش فناوری اطلاعات در سامانه های C4I»، فصل نامه پژوهشیار، ویژه نامه C4I، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

(۳)- تافلر، الوین و تافلر، هیدی، (ترجمه مهدی بشارت) (۱۳۷۴): «جنگ و پاد جنگ»، چاپ اول، تهران، انتشارات اطلاعات.

(۴)- حقیری، علی اصغر و ستاریخواه، علی (۱۳۸۴): «سامانه فرماندهی و کنترل به عنوان عامل برترساز در نیروهای مسلح»، فصلنامه مطالعات دفاعی استراتژیک، دانشگاه عالی دفاع ملی، شماره ۲۳ و ۲۴.

(۵) سعیدی کیا، علی اکبر (۱۳۸۰): «فرآیند تحول سازمان در اثر فناوری اطلاعات»، ماهنامه روش، ویژه نامه فناوری اطلاعات، تهران.

(۶)- عباسی اشلقی، مجید (۱۳۸۵): «امنیت ملی در عصر اطلاعات»، فصلنامه راهبرد دفاعی، مرکز تحقیقات راهبردی دفاعی، شماره ۱۲.

(۷)- عبدا... خانی، علی (۱۳۸۴): «حفاظت از زیرساخت های حیاتی اطلاعات»، فصلنامه مطالعات دفاعی استراتژیک، دانشگاه عالی دفاع ملی، شماره ۲۳ و ۲۴.

(۸)- طرح فراسازمانی فاوا نیروهای مسلح (۱۳۸۵): «نقش فناوری اطلاعات در جنگ های آینده»، چاپ اول، تهران، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

(۹)- قاضی زاده فرد، سید ضیاء الدین (۱۳۸۵): «جنگ اطلاعاتی و فناوری اطلاعات در جنگ های آینده»، دوماهنامه اندیشه مدیران، شماره ۷ و ۸، خانه مدیران صنایع دفاعی، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

(۱۰)- قاضی زاده فرد، سید ضیاء الدین (۱۳۸۶): «ویژگی ها و ابعاد جنگ های اطلاعاتی درجنگ‌های آینده»، مجموعه مقالات پنجمین همایش تخصصی گروه مهندسی صنایع دانشکده

علوم و مهندسی دانشگاه امام حسین (ع) تحت عنوان «کاربردهای فناوری اطلاعات و ارتباطات در مهندسی صنایع (به ویژه در صنایع نظامی و نیروهای مسلح».

(۱۱)- کاستلز، مانوئل (ترجمه افشین خاکباز و احد علیقلیان) (۱۳۸۰): «عصر اطلاعات: اقتصاد، جامعه و فرهنگ، ظهور جامعه شبکه ای»، انتشارات طرح نو، چاپ اول، تهران.

(۱۲)- مرادی، بیژن (۱۳۷۹): «اطلاعات و نقش جنگ الکترونیک در C4I»، فصل نامه پژوهشیار، ویژه نامه C4I، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

(۱۳)- نقش بندی ، افشین (۱۳۷۹): «نقش کامپیوتر در سیستم های C4I»، فصل نامه پژوهشیار، ویژه نامه C4I، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

(۱۴)- والتز، ادوارد (ترجمه رنجبر و دیگران)، (۱۳۸۵): «جنگ اطلاعات، اصول و عملیات»، طرح فراسازمانی فاوا نیروهای مسلح، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

ب) انگلیسی

1) Davis, Norman (1996): "An Information – Based Revolution in Military Affairs", strategic review, 24 (1), www.Rand.org/Publication/Mr/Mr880/Mr880,ch4.pdf

2) Goldman, Emily O. (2004): "National Security in the Information Age", London: Frank Cass, Pges 238.

3) Roger C. Molander & A.S. Riddile & Peter Wilson (1996): "Strategfic Information Warfare: A New face of war", Santa Monica, Calif, Rand, Mr-661-osd, WWW.Rand.org/Publication/Mr/Mr661.

4) Rona, P. Thomas (1996): "Information Warfare : An Age- Old Concept with new insight", Defense intelligence Journal , Spring, P53.