مجله سیاست دفاعی
سال بیستم، شماره ۷۹، تابستان ۱۳۹۱

ارائه چارچوبی برای مفهوم‌سازی رزم اطلاعاتی

علیرضا فرشچی [۱]
احسان مرآتی [۲]

تاریخ دریافت مقاله: ۱۳۹۱/۱۲/۱۰
تاریخ تأیید مقاله: ۱۳۹۱/۰۳/۲۰
صفحات مقاله: ۱۲۹ – ۹۷

چکیده:

قابلیت‌های روز افزون فناوری اطلاعات موجب گردیده تا حوزه‌ی دفاعی به‌عنوان یکی از حوزه‌های حساس و مهم، پیوسته به دنبال توسعه و به‌کارگیری قابلیت‌های بروز فناوری اطلاعات باشد. این امر موجب شده تا گاهی حوزه‌ی دفاعی مبدع بروزترین فناوری‌های اطلاعاتی باشد، از طرفی، محققین به‌منظور بسترسازی توسعه‌ی کاربردهای فناوری اطلاعات در حوزه‌ی دفاعی به مفهوم‌سازی کاربردهای مربوطه پرداخته‌اند. از این رو، حضور و ظهور فناوری اطلاعات در حوزه‌ی دفاعی موجب شکل‌گیری مفاهیمی نظیر رزم سایبری [۳]، رزم مبتنی بر شبکه [۴] و رزم الکترونیک [۵] شده است. بر اساس ادبیات، اکثر این اصطلاحات در حوزه‌ی رزم اطلاعاتی [۶] قرار می‌گیرند. با این حال، از لحاظ نظری چگونگی ارتباط بین مفاهیم گوناگون و چگونگی پوشش دان آنها توسط رزم اطلاعاتی به‌خوبی تبیین نشده است. از این رو، پژوهش حاضر به‌واسطه‌ی مطالعه و تحلیل مدل‌ها و مفاهیم موجود در حوزه‌ی رزم اطلاعاتی و مقایسه و مطالعه‌ی تطبیقی آنها به تبیین چارچوبی چند بُعدی برای مفهوم‌سازی رزم اطلاعاتی پرداخته است. این چارچوب تمامی اصطلاحات موجود در حوزه‌ی رزم اطلاعاتی را پوشش داده و به تبیین و تحلیل ابعاد گوناگون و زیربنایی رزم اطلاعات می‌پردازد. این چارچوب، می‌تواند به‌عنوان مبنایی برای نقد پژوهش‌های حوزه‌ی رزم اطلاعاتی مورد استفاده قرار گرفته و به آشفتگی مفاهیم حوزه‌ی رزم اطلاعاتی نظم بخشد که این نظم به نوبه‌ی خود منجر به شکل‌گیری تفکر ساختاریافته در حوزه‌ی رزم اطلاعاتی و پیشرفت آن در ابعاد گوناگون زیربنایی می‌گردد.

---

۱ – رئیس مرکز مطالعات دفاعی و امنیت ملی.
۲ - دانشجوی دکترای مدیریت سیستم، دانشکده مدیریت، دانشگاه تهران.

3 – Cyber Warfare
4 – Net-Centric Warfare
5 – Electronic Warfare
6 – Information Warfare

* * * * *

واژگان کلیدی

فناوری اطلاعات، رزم اطلاعاتی، رزم دانش محور، رزم اطلاعات راهبردی، رزم مبتنی بر شبکه.

مقدمه

فناوری اطلاعات[1] از سال ۱۹۸۰ میلادی تاکنون تغییر و تحولات بسیاری را تجربه نموده که از جمله آنها می‌توان به تغییرات سریع سیستم‌های کامپیوتری و شبکه‌های ارتباطات برخط[2] اشاره نمود. برخی روندهای گذشته در جهت پیشبرد فناوری و آنچه که امروز در اختیار داریم، حرکت کرده‌اند و برخی اثر و حرکت معکوس داشته‌اند و لذا پس از مدت کوتاهی ناپدید شده‌اند (Silberglitt et al., 2006). امروزه، فناوری اطلاعات مفهومی گسترده است که حوزه‌های متنوعی را در خود جای داده است و به‌دلیل برخورداری از قابلیت‌های گوناگون، در حوزه‌های مختلف مورد استفاده قرار گرفته است. از طرفی، به دلیل اهمیت اطلاعات در حوزه‌ی دفاعی، به‌کارگیری فناوری اطلاعات در حوزه‌ی دفاعی توجیه‌پذیر می‌باشد و کشورهای مختلف با وجود صرف هزینه‌های زیاد به به‌کارگیری جدیدترین دستاوردهای فناوری اطلاعاتی در حوزه‌ی دفاعی ترغیب شده‌اند (Janczewski and Colarik, 2008). در فضای رزم، اجرای موفق یک عملیات نظامی مستلزم اطلاع حاضرین در صحنه از اهداف عملیات، روش دستیابی به آنها، قابلیت‌ها و فعالیت‌های دشمن، شرایط آب و هوایی و منطقه، میزان محرمانگی عملیات و سایر عواملی است که ممکن است هر لحظه تغییر کنند. الزام به مدیریت مؤثر اطلاعات و همچنین لزوم مورد هدف قرار دادن سیستم‌ها و منابع اطلاعاتی دشمن موجب شکل‌گیری مفهومی به نام رزم اطلاعاتی گردیده است (Janczewski and Colarik, 2008).

1 – Information Technology (IT)
2 – Online

رزم اطلاعاتی یکی از حوزه‌های مطالعاتی نسبتاً جدید است. دکتر توماس رونا[1] در سال ۱۹۷٦ میلادی به واژه‌ی رزم اطلاعاتی اشاره نمود (Halpin et al., 2006). از آن زمان به بعد، تعاریف مختلفی با تأکید بر جنبه‌های نظامی ارائه شد. امروزه، منظور از جنگ اطلاعاتی یا جنگ سایبر، به تعارضات سیاسی، اقتصادی، حقوقی، امنیتی، مدنی و نظامی است. تعاریف دیگر ارائه شده از رزم اطلاعاتی، آن را اقداماتی با هدف حفاظت، بهره‌گیری، تخریب، تحریف، یا نابود کردن اطلاعات یا منابع اطلاعاتی و کسب مزیت نسبت به دشمن یا حصول به هدفی خاص می‌دانند. کرونین و کراوفورد[2] (۱۹۹۹) چارچوبی را برای رزم‌های اطلاعاتی ارائه نموده‌اند که از حیطه‌ی نظامی فراتر رفته است. آنها بر این باورند که نبردهای این‌چنینی شدت خواهند گرفت و مشکلات اجتماعی و چالش‌های حقوقی جدیدی را به جامعه تحمیل خواهند کرد.

هنوز در مورد نقش و اثربخشی بالقوه‌ی اطلاعات و فناوری‌های اطلاعاتی در فضای نبرد، بحث و اختلاف‌نظر وجود دارد. برخی نقش اطلاعات و سیستم‌های اطلاعاتی را کار کردن روی ذهن افراد (عام و خاص) و قانع ساختن آنها به همراهی می‌دانند تا از این طریق، نیاز به تقابل فیزیکی به حداقل برسد. حامیان این دیدگاه می‌کوشند به «تعالی برتر»[3] و تفوق مورد نظر «سان تزو»[4] که همان «شکستن مقاومت دشمن، بدون جنگیدن» است، دست یابند. زافرانسکی[5] (۱۹۹۵) این دیدگاه را توسعه داده و معتقد است هدف راهبردی می‌تواند به‌جای مواضع فیزیکی دشمن، شناخت‌شناسی[6] (سیستم باورها و عقاید) او باشد و از نیروی نظامی به‌عنوان ابزار ثانویه بهره‌گیری شود.

یکی از اثرات به‌کارگیری فناوری اطلاعات در فضای رزم، گسترش میدان جنگ ماورای مرزهای سنتی آن است. سلاح‌ها و اهداف اطلاعاتی بخش‌مهمی از سرمایه‌های زیرساختی ملت‌ها را

1 – Thomas Rona
2 – Cronin & Crawford
3 – Supreme excellence
4 – Sun Tzu
5 – Richard Szafranski
6 – epistemology

تشکیل می‌دهند. در گذشته ارتش‌ها، با سلاح‌های نظامی به اهداف نظامی حمله می‌کردند؛ اما در نبرد اطلاعاتی همه‌ی منابع و فرآیندهای اطلاعاتی یک ملت می‌توانند سلاح و اهداف بالقوه جنگی به‌شمار روند. برخی دیگر نیز حمله‌ی اطلاعاتی و نشانه رفتن ادراک و باورهای شخصی را اقدامی تکمیلی در عملیات نظامی می‌دانند و آن را جایگزین حمله‌ی نظامی نمی‌دانند، بلکه مکمل آن تلقی می‌کنند. اطلاعات می‌تواند کاربرد یک سلاح را داشته باشد و استراتژیست‌ها باید با دقت و احتیاط از آن بهره گیرند. استراتژیست‌ها باید برای استفاده از اطلاعات به موازات سلاح‌های رایج دیگر برنامه‌ریزی نمایند و پیش از انجام عملیات نظامی و حمله فیزیکی، از آن بهره گیرند (Cronin & Crawford, 1999). در واقع، طیفی از انواع رزم‌ها وجود دارد که هر کدام برای دستیابی به اهداف خود نیازمند ترکیب خاصی از نیروهای فیزیکی و نیروهای اطلاعاتی هستند. جنگ‌های روانی و اقتصادی از جمله نبردهایی هستند که ابزارهای اطلاعاتی و شبکه‌های جهانی، آنها را به بهترین وجه پیاده‌سازی می‌کنند. در مجموع اکثر ادبیات مرتبط با جنگ‌های اطلاعاتی و سایبری به ابعاد نظامی آن پرداخته‌اند. در حالی که، رزم اطلاعاتی خود را به حوزه‌های غیرنظامی نیز توسعه داده است (Cronin & Crawford, 1999).

با همه‌ی این اوصاف، یکی از نکات قابل تأمل در حوزه‌ی رزم اطلاعاتی، مفاهیم متعددی است که برای تبیین چیستی رزم اطلاعاتی و تشریح ابعاد آن ذکر گردیده است. پژوهشگران از اصطلاحاتی نظیر رزم سایبری، رزم مبتنی بر شبکه، رزم مبتنی بر دانش و رزم الکترونیک برای تبیین رزم اطلاعاتی بهره گرفته‌اند. این امر موجب آشفتگی در مفاهیم مطروحه و عدم تبیین دقیق چیستی و ابعاد رزم اطلاعاتی گردیده است. از این رو، این مقاله به ارائه‌ی چارچوبی برای رزم اطلاعاتی می‌پردازد که در آن با تبیین ابعاد زیربنایی رزم اطلاعاتی و پوشش دادن اصطلاحات مطروحه در حوزه‌ی رزم اطلاعاتی، به مفهوم‌سازی بنیادین رزم اطلاعاتی پرداخته شده است.

اطلاعات در فضای رزم

اندیشمند چینی «سان تزو» به اهمیت اطلاعات دقیق و به‌موقع برای فرماندهان نظامی اشاره نموده است. او در این گفتار کوتاه به ابعادی از رزم اشاره نموده که اطلاعات نقش مهمی در تصمیم‌گیری‌های مربوط به آنها دارد؛ اولین آنها شناخت دشمن است (Tzu, 1971).

شناخت دشمن

یک فرمانده‌ی جنگی به مجموعه‌ای از اطلاعات مختلف در مورد دشمنی که در مقابلش صف‌آرایی کرده، نیاز دارد: تعداد نیروهای دشمن، نوع و تعداد تجهیزات جنگی در اختیار دشمن، موقعیت مکانی آنها، آمادگی آنها برای مبارزه، مشخصات پایگاه تدارکات[1] آن، اهداف مدنظر فرمانده‌ی دشمن و موارد این‌چنینی. هرچه تصویر کامل‌تر و دقیق‌تری از دشمن موجود باشد، برنامه‌ریزی برای عملیات و چیدمان نیروها و منابع به نحو بهتری صورت خواهد گرفت و آمادگی نیروها برای مقابله با حوادث و وقایع آتی بیشتر خواهد بود.

ماهیت رزم ایجاب می‌کند که کسب دانش در خصوص دشمن همواره با نقایص فراوان همراه باشد. کلاوزویتس[2] نیز با این باور موافق است. وی بیان می‌دارد که بخش زیادی از اطلاعات گردآوری شده در جریان جنگ‌ها متناقض هستند و بخش قابل‌توجه دیگری غلط بوده و به باقیمانده اطلاعات که بخش اعظم آن نیز می‌باشد، با تردید نگریسته می‌شود. کلاوزویتس این اطلاعات را به دیدن صحنه‌ای از پشت مه یا زیر نور سپیده دم تشبیه می‌کند. او بر این باور است که مشکل بودن گردآوری اطلاعات درست، یکی از منابع اصلی اصطکاک و حساسیت در جنگ‌ها به شمار می‌رود.

برای ارزیابی اعتبار دیدگاه‌های کلاوزویتس نگاهی به کیفیت اطلاعات در دسترس فرماندهان نیروهای چندملیتی متفقین در جنگ خلیج می‌اندازیم. هیچ نیروی نظامی تاکنون اطلاعاتی در این حد کامل و روشن از دشمن خود در اختیار نداشته است: طی پنج ماه پشتیبانی توان رزمی نیروها و شش هفته نبرد، متفقین در مقابله با نیروهای عراقی از حسگرهای هوابرد، گیرنده‌های امواج الکترونیک، و نیروهای اطلاعاتی ویژه‌ای بهره‌مند بودند. با این حال، پس از جنگ مشخص شد، فرماندهان متفقین و تحلیل‌گران کلیدی آنها، تصوری نادرست از دشمن داشته‌اند و در مواردی کلیدی مرتکب اشتباهاتی در ارزیابی شده‌اند. آنها قدرت نیروی زمینی عراق را به نحو درستی برآورد نکرده بودند و توان عراق در تولید

1 – Logistic
2 – Clausewitz

سلاح‌های کشتارجمعی را بسیار دست‌کم گرفته بودند. همچنین در یافتن و هدف‌گیری موشک‌اندازهای متحرک زمین به زمین عراقی که موجب سردرگمی نیروهای آنها شده بود، با مشکل مواجه شدند و توانایی صدام برای حفظ قدرت را دست‌کم گرفته بودند. فرماندهان نظامی در طول تاریخ همواره با عدم قطعیت‌های این‌چنینی و شرایطی بسیار مبهم‌تر از این مواجه بوده‌اند و باید آمادگی مقابله با این ابهامات را داشته باشند.

شناخت خود

به همان میزان که شناخت دشمن مهم است، شناخت دقیق توانایی‌ها، قابلیت‌ها، محدودیت و موقعیت دقیق مکانی نیروهای خودی حایز اهمیت است. دشمن همواره در تلاش برای پنهان کردن اقدامات خود است، اما نیروهای خودی چنین انگیزه‌ای ندارند. با این حال، شرایط ویژه‌ی جنگ ممکن است فرماندهان را در ارزیابی نیروهای خود دچار خطا نماید. فرماندهان عالی‌رتبه اغلب نمی‌توانند تصور دقیقی از رزمی داشته باشند که در فاصله‌ی چند صد مایلی[1] آنها رخ می‌دهد. درک غلط فرماندهان از نیروهای تحت فرمان و شرایط آنها در رده‌های پائین‌تر نیز رخ می‌دهد. یکی از مشکل‌سازترین ابهامات فرماندهان عملیات نظامی، ضعف اطلاعات آنها از محل دیگر واحدهای خودی در منطقه‌ی جنگی است. در شرایطی که تشخیص نیروهای خودی از دشمن مشکل می‌شود، بدون خطر کردن در مورد نیروهای خودی نمی‌توان از آتش پشتیبانی بهره‌گرفت. برای نمونه؛ نیروهای زمینی و هوایی ایالات متحده رویه‌های عملیاتی خاصی برای کنترل آتش در حوالی نیروهای خودی دارند؛ این موارد، تعیین حدود مشخص برای آتش خودی و ثبت علائم مشخصه روی ماشین‌آلات و ادوات نظامی خودی را شامل می‌شوند. علی‌رغم درنظر گرفتن این تمهیدات و موارد دیگری از این دست، هنوز روشی برای حصول اطمینان قطعی از عدم وقوع تلفات خودی وجود ندارد.

1 – Mile

شناخت زمین، شناخت هوا

آشنایی با زمین و جغرافیای منطقه‌ی عملیات، همواره از اولویت‌های برتری نیروهای نظامی بوده است. تهیه‌ی نقشه‌ای مناسب از محل وقوع جنگ همواره از چالش‌های اصلی فرماندهان نظامی و کارکنان آنها بوده‌اند. در اواسط دهه‌ی ٦٠ میلادی هنگامی که نخستین نیروهای نظامی ایالات متحده وارد ویتنام شدند، نقشه‌های راه شرکت‌های نفتی تا مدت‌ها بهترین نقشه‌هایی بودند که واحدهای نظامی در اختیار داشتند. با وجود این‌که نقشه‌های خوبی تهیه شده بودند، گاه فرماندهان نظامی در ویتنام خود را در شرایطی پیش‌بینی نشده و منطقه‌ای ناآشنا می‌یافتند.

کنترل نیروها

کنترل – توانایی هدایت فعالیت‌های نیروها در میدان جنگ–، یکی دیگر از ابعاد فضای رزم است که اطلاعات در آن نقشی کلیدی ایفا می‌کند. غالبا گفته می‌شود که هیچ نقشه جنگی نمی‌تواند از نخستین مواجهه خود با دشمن جان سالم به در ببرد. بنابراین فرماندهان باید قادر باشند در هر لحظه از نبرد با توجه به شرایط تاکتیکی، نیروهای خود را متمرکز کنند، از فرصت‌ها استفاده کنند و از نقاط آسیب‌پذیر خود پشتیبانی و حفاظت کنند.

با توجه به اهمیت چشمگیر اعمال کنترل روی نیروهای تحت فرمان، در گذشته محدودیت‌های کنترلی متغیر اصلی تعیین کننده سازمان نیروهای نظامی و تاکتیک‌های مورد استفاده آنان بود. پیش از توسعه‌ی ابزارهای ارتباطی راه دور، حیطه‌ی کنترل یک فرمانده جنگی به افراد اطرافش که توانایی شنیدن صدای او را داشتند، محدود می‌شد. ارتباطات مدرن امکان گسترش این حیطه را فراهم نموده‌اند. البته در میدان نبردی که همه چیز به سرعت در حال وقوع و تغییر است، تجهیزات ارتباطی مدرن نیز نمی‌توانند متضمن کنترل دقیق حرکات نیروها توسط فرمانده باشند. با وجود توسعه‌ی ارتباطات رادیویی، پیام‌های دیجیتال، نقشه‌های الکترونیک و علائم قراردادی در میان افراد، باید همواره درنظر داشت که فرمانده تاکتیکی یک عملیات تنها یک نفر است و ظرفیت‌های شناختی محدودی دارد.

سرعت و قاطعیت

در اختیار داشتن سیستم‌های کنترلی و اطلاعات مناسب یک مقوله است و بهره‌گیری عملی از آنها مقوله دیگری است. به طور کلی، هرچه فرد به میدان نبرد نزدیک‌تر باشد، زمان برای او حساس‌تر می‌شود. ثانیه‌ها برای نیروهای زمینی درگیر در جنگ آتش یا نیروی هوایی درگیر در یک عملیات هوایی، اهمیت دارد. در یک نبرد یا لشکرکشی، فرماندهان عملیاتی در سطوح میانی تنها چند ساعت برای اتخاذ تصمیمات مهم اعم از نحوه تخصیص نیروها، فرصت دارند. در چنین شرایط حساسی، ارزش اطلاعات کسب شده از دشمن می‌تواند به سرعت دستخوش تغییرات عظیم شود. موفقیت در نبرد تا حد زیادی به سرعت عکس‌العمل در مقابل دشمن وابسته است. این سرعت عمل شامل چهار فعالیت متوالی می‌باشد: مشاهده، درک وضعیت و جهت‌گیری، تصمیم‌گیری، عمل کردن. در جنگ‌ها عموماً طرفی که بتواند این اعمال را بهتر و سریع‌تر به انجام برساند، صرف‌نظر از وضعیت عملیاتی و تاکتیکی خود، برنده میدان خواهد بود.

رزم اطلاعاتی: ظهور فناوری اطلاعات در حوزه دفاعی

بحث در مورد پیشرفت‌های سریع اخیر در مدیریت اطلاعات حوزه دفاعی، اغلب به مباحث پیچیده‌ای وارد می‌شود، عباراتی مانند «فضای نبرد مجازی» و «جنگ سایبر» در ادبیات ناپدید می‌شوند و جای خود را به واژه‌هایی مانند «فضای رزم شبکه محور» می‌دهند. این امر موجب بروز شک و تردید در متخصصین نظامی می‌شود؛ که البته با جدید بودن این مباحث و نبود تجربه در این زمینه، قابل توجیه است و گاهی درک عملکرد سیستم‌های جدید و تأثیر آنها در نحوه‌ی اجرای عملیات نظامی مشکل است. روشن است پیشرفت‌های فناوری اطلاعات نظامی در بسیاری از حوزه‌ها واقعی و کاربردی است و منافع شناخته‌شده‌ای دارد. در حال حاضر، برنامه‌ریزان نظامی با این چالش مواجهند که چگونه فناوری‌های جدید اطلاعاتی و قابلیت‌های آن را در عملیات نظامی پیاده‌سازی نمایند.

امروزه فناوری اطلاعات به مهم‌ترین عامل ایجاد کننده قدرت نظامی تبدیل شده است (Rattray, 2001). تا چندی پیش نظامیان تنها برای تقویت قابلیت‌های موجود خود از فناوری اطلاعات بهره می‌گرفتند؛ اما همان‌گونه که فناوری اطلاعات موجب تغییر همه رویه‌ها در کسب‌وکارهای تجاری گردید، تغییر روش‌های کاری دفاعی را نیز به دنبال داشته است. در نتیجه، انقلاب اطلاعاتی و تأثیر آن بر عملیات و نیروهای نظامی، معیارهای ارزیابی قدرت نظامی متحول گردیده است. اندازه ارتش‌ها و میزان سلاح‌های سنگین مورد استفاده آنها، تعداد هواپیماها و کشتی‌های نظامی دیگر اهمیت سابق را ندارند. عملکرد (شامل دقت، قابلیت اطمینان و میزان مرگبار بودن) سلاح‌های شخصی به‌کمک علم میکروالکترونیک بهبود یافته است، اما زمانی ارزشمند است که به‌صورت هماهنگ با سایر سلاح‌ها عمل کند. توسعه‌ی ارتباطات ما را قادر ساخته است تا حسگرها، سلاح‌ها و سیستم‌های فرماندهی را در قالب سپاهی یکپارچه درآورده و برآیند کل را به چیزی بیشتر از مجموع عملکرد تک‌تک این اجزاء ارتقا دهیم.

استفاده یکپارچه و هماهنگ از سلاح‌ها، حسگرها، و سایر سیستم‌های نظامی به توانمندی نیروهای نظامی در انجام فعالیت‌های کنترل، ارتباطات، محاسبات، فرماندهی، دیده‌بانی و شناسایی، وابسته است. نظامیان با بهره‌گیری از این ابزارها می‌توانند کلیه حرکات دشمن را شناسایی و ردیابی کنند و نیروهای خود را برای نشان دادن عکس‌العمل مناسب هماهنگ کنند تا از این طریق تعیین‌کننده نتیجه جنگ باشند (Ventre, 2011).

رابطه معکوس فاصله و دقت به واسطه‌ی فناوری اطلاعات در حال از بین رفتن است. سلاح‌های مرگبار با کمک فناوری‌های شناسایی و تعقیب واحدهای دشمن، به تخریب سریع و سیستماتیک نیروهای دشمن و زیرساخت‌های نظامی آنها منجر می‌شوند. نیاز به پرواز هواپیماهای دارای سرنشین در محدوده‌ی استقرار دشمن کاهش یافته و سلاح‌های دارای کنترل از راه دور برای شناسایی و تخریب اهداف مورد نظر استفاده می‌شوند.

فناوری اطلاعات امکان جنگ یکپارچه و مشترک را فراهم می‌نماید که می‌تواند مزیت جنگی عظیمی به‌شمار رود. به‌جای حمل سلاح‌های مختلف از طریق زمین، هوا و دریا به صورت جداگانه، نیروهای دخیل در نبرد مشترک می‌توانند به‌صورت یکپارچه اقدام به اجرای عملیات هماهنگ نمایند.

این امکان بالقوه وجود دارد که هریک از قابلیت‌های نیروهای مشترک، بنابر اولویت، با اجزای مختلف ارتش دشمن مقابله نمایند. با تجمیع قابلیت‌های مختلف نظامیان شرکت کننده در نبرد مشترک، شانس دشمن برای دفاع از نیروها و مواضعش به حداقل می‌رسد (Ventre, 2011).

تدارکات دفاعی به واسطه‌ی فناوری اطلاعات بخش خصوصی و روش‌های کاری آن، ناب و سریع‌تر شده‌اند. رهبران ارتش ایالات متحده و منتقدان آن، هنوز در پیچ‌وخم مشکلات بازسازی ساختار و کوچک سازی تأسیسات و انبارهای نظامی عظیمی هستند که در گذشته ایجاد شده است؛ اما تا نیمه راه را طی کرده‌اند. بیشتر ارتش‌های دیگر جهان هنوز فاصله زیادی با این وضعیت دارند و تأسیسات قدیمی آنها بجای پشتیبانی واقعی از عملیات نظامی، موجب اتلاف منابع می‌شوند. فناوری اطلاعات این امکان را فراهم می‌نماید که بهره‌وری تأسیسات دفاعی افزوده شده و تدارکات، مدیریت منابع و آموزش بهبود یابد. در مجموع، فناوری اطلاعات، سیستم‌های نظامی را به‌طور کلی متحول نموده است (Ventre, 2011).

فناوری اطلاعات که به صورت فیزیکی شامل مجموعه‌ای از سخت‌افزارها، نرم‌افزارها و سیستم‌ها و ابزارهاست، تنها دلیل برتری نظامی ابرقدرتها نیست و نباید نقش مزیت‌های ذاتی جامعه را در آن نادیده گرفت. امروزه وجود نیروهای بسیار شایسته اطلاعات محور، به بخشی جدایی‌ناپذیر و کلیدی در موفقیت‌های نظامی کشورها تبدیل شده است و یافتن چنین افرادی در اقتصادهای آزاد و جوامع باز، امکان‌پذیر است. جوامعی که از چنین ویژگی‌هایی برخوردار نباشند تنها می‌توانند سلاح‌ها و سیستم‌های جدید را خریداری نمایند، اما محکوم به استفاده از نیروهای درجه دو و تأسیسات عصر صنعتی هستند که قطعاً توان نظامی آنها را محدود می‌کنند. نظام‌های جامعه‌محور در تأمین همزمان دو جزء «انسان» و «ماشین» برای سیستم‌های اطلاعاتی نظامی خود توفیق بیشتری دارند.

در آینده، سلاح‌های کشتار از راه دور –زمین، دریا و هوا– موفقیت ارتش‌های مجهز به فناوری اطلاعات را تضمین خواهد کرد. اما نقش نبردهای کوچک و پیاده‌نظام‌های پراکنده و پنهان شدن و غافلگیر کردن دشمن را نباید نادیده گرفت؛ که هیچ‌یک نیازی به فناوری اطلاعات ندارند. آیا راهبردهای این‌چنینی با این ایده که ملت‌ها باید در فناوری اطلاعات قوی شوند، در تضاد است؟ پاسخ منفی است. با در نظر داشتن این واقعیت که تحولات مذکور در سیستم‌های نظامی هنوز مراحل اولیه خود را می‌گذرانند، به موازات

توسعه‌ی کاربردهای فناوری اطلاعات، مجموعه‌ای رو به گسترش از راهبردهای مقابله با حملات نظامی بی‌اثر خواهند شد. تأسیسات نظامی، پادگان‌های نظامی و پایگاه‌های استقرار نظامیان از آسان‌ترین اهداف قابل شناسایی و تخریب هستند و از میان بردن آنها با کمک نیروهای مسلط به فناوری اطلاعاتی و ابزارهای دقیق و سریع مورد استفاده آنها، بیش از پیش تسهیل می‌شود (Rattray, 2001).

با وجود همه این موارد، احتمال آن وجود دارد که نیروهای نظامی در عملیات خود از فناوری‌های رایج بهره‌گیری نکنند و همچنان خطرساز و تهدیدکننده باشند. با این حال هر ارتشی که بخواهد در سطح منطقه‌ای یا جهانی قدرت بگیرد یا قصد مقابله با نیروهای قدرت‌های برتر را داشته باشد، باید خود را به فناوری اطلاعات و قابلیت‌های ناشی از آن مجهز کند. برای این کار لازم است فضایی مردمی و اقتصادی آزاد وجود داشته باشد تا فرصت برای رشد فناوری جدید و دانش مرتبط با آن فراهم گردد (Gompert, 1999).

بررسی ادبیات رزم اطلاعاتی، نمایانگر روندهایی (جدول شماره‌ی ۱) است که رزم اطلاعاتی را از حیطه‌ی نظامی خارج نموده و وارد مسائل مدنی نموده است. در ادامه هر یک از این روندها تشریح شده است.

جدول شماره‌ی ۱ - روندهای رزم اطلاعاتی (Janczewski and Colarik, 2008)

ویژگی‌های رزم اطلاعاتی	۱۹۹۰	۲۰۰۵
۱- حوادث مرتبط با کامپیوتر	۲۵۲ حادثه	۱۳۷۵۲۹ حادثه (سال ۲۰۰۳)
۲- موانع ورود در مقابل حمله‌های سایبر	موانع زیاد	موانع کم
۳- انواع سلاح‌های سایبر	انواع محدود، دسترسی کم	متنوع، دسترسی زیاد
٤- کشورهای بهره‌مند از برنامه‌های رزم سایبر	معدود	بیش از ۳۰
٥- وابستگی اقتصادی به زیرساخت‌های اطلاعاتی	بخشی، وابستگی رو به افزایش	وابستگی بسیار زیاد
٦- هدف اصلی در تعارضات اطلاعاتی	نظامی و خصوصی	افزایش اهداف خصوصی
۷- کاربرد فناوری سایبری در مدیریت ادراکات افراد	تلویزیون، رادیو	رسانه‌های متنوع و جهانی
۸- کاربرد فناوری سایبری در جاسوسی تجاری	کم (قابل چشم‌پوشی)	به میزان قابل توجه و رو به افزایش
۹- کاربرد فناوری سایبری در جنایات سازمان‌یافته	کم (قابل چشم‌پوشی)	به میزان قابل توجه و رو به افزایش
۱۰- کاربرد فناوری سایبری در مقابل افراد حقیقی و کسب‌وکارهای کوچک	کم (قابل چشم‌پوشی)	به میزان قابل توجه و رو به افزایش

حوادث مرتبط با کامپیوتر توسعه یافته‌اند: امروزه حوادث امنیتی بسیار رایج هستند، سازمان‌ها و مؤسسات خصوصی هدف بسیاری از حمله‌های سایبری هستند، جامعه و عموم مردم از بسیاری از تهاجمات این‌چنینی بی‌اطلاع می‌مانند. تعداد حوادث گزارش شده از ۷ حادثه در سال ۱۹۸۸ به ۱۳۷۵۲۹ در سال ۲۰۰۳ رسیده است. با وجود این‌که تعداد حوادث گزارش شده زیاد است، این احتمال وجود دارد که بسیاری از حوادث گزارش نشده باشند. پاسخ‌دهندگان به نظرسنجی‌ها بر این باورند که حوادث این بخش بیش از تعداد گزارش شده توسط شرکت‌ها به مشتریان و سهامداران و شرکای تجاری آنهاست. برای مثال، در سال ۲۰۰۵ فقط ۲۰٪ پاسخ‌دهندگان اظهار داشته‌اند که به دلیل نگرانی از ایجاد شهرت و تبلیغات منفی اقدام به گزارش حوادث به مراجع قانونی نموده‌اند (Gordon et al., 2005).

موانع ورود در مقابل حمله‌های سایبری کم هستند: برای استفاده اثربخش از نسل‌های اول سلاح‌های سایبری نیاز به دانش فنی وجود داشت. برای مثال، برخی هکرهای دهه‌ی ٦٠ میلادی از دانشجویان دانشگاه ماساچوست[1] بودند. در دهه‌ی ۷۰ میلادی هکرها افرادی بسیار با انگیزه و باهوش بودند که از دانش فنی بالایی برخوردار بودند و اغلب در مراکز کامپیوتری دانشگاه‌ها مشغول به کار بودند (Jones et al., 2002). در اوایل دهه‌ی ۹۰ میلادی شرایط عوض شد؛ موانع فنی به مرور حذف شدند و تعاملات کاربری از طریق صفحات گرافیکی صورت گرفت. در اواخر دهه‌ی ۹۰ یک اتفاق بزرگ رخ داد. گروهی از نوجوانان هکر تحت سرپرستی جوانی ۱۸ ساله، به تعدادی از کامپیوترهای دولتی و نظامی نفوذ کردند. این اتفاق، هشداری بود که همگان را متوجه خطر موجود از جانب افراد متخصص و نسبتاً غیرمتخصص نمود. در سال ۱۹۹۹ میلادی، مدیر آژانس اطلاعات مرکزی آمریکا[2] در کنگره اذعان داشت تروریست‌ها و سایر افراد دریافته‌اند رزم اطلاعاتی می‌تواند روشی کم‌هزینه برای دستیابی به منافع آنها باشد. تنها تا سال ۲۰۰۲ میلادی متخصصین امنیتی بیش از ٦ هزار سایت هکر را شناسایی کرده بودند که ابزارهای هک و نفوذ را در اختیار داشتند (Jones et al., 2002).

1 – Massachusetts
2 – Central Intelligence Agency (CIA)

ظهور انواع خطرناکی از سلاح‌های سایبری: نخستین جامعه‌ی اینترنتی هکرها در حدود سال ۱۹۸۰ میلادی تشکیل شد و به طرح و انتشار تکنیک‌ها و نرم‌افزارهای آنها کمک کرد. حمله‌ی اینترنتی ۷ فوریه سال ۲۰۰۰ میلادی به‌وسیله‌ی همین نرم‌افزار انجام شد و منجر به از کار افتادن تعداد زیادی از سایت‌های اینترنتی شد. سازمان تحقیقات دفاعی انگلستان اعلام نمود که تروریسم سایبری در این کشور میلیون‌ها پوند خسارت به کامپیوترها وارد ساخته است (Rhem, 2005).

دسترسی بسیاری از کشورها به فناوری رزم اطلاعاتی: در اوایل دهه‌ی ۹۰ میلادی تنها تعداد محدودی از کشورها از قابلیت رزم اطلاعاتی بهره‌مند بودند. در سال ۲۰۰۱ میلادی تعداد آنها به بیش از ۳۰ کشور رسید که از جمله آنها می‌توان به هند، چین، تایوان، ایران، رژیم اشغالگر قدس، فرانسه، روسیه و برزیل اشاره نمود. نتایج بررسی‌های میدانی حاکی از این است که ۲۸٪ پاسخ‌دهندگان، این احتمال را می‌دهند که از سوی دولت‌های دیگر حمله‌های سایبری به سیستم‌های آنها انجام شود. چین یکی از کشورهایی است که قابلیت‌های خود را در حیطه‌ی رزم اطلاعاتی گسترش داده است (Gordon et al., 2005).

افزایش وابستگی اقتصادی به زیرساخت‌های اطلاعاتی: جامعه امروز مراحل کشاورزی و صنعتی را پشت سر گذاشته است و در حال حاضر فرهنگ مبتنی بر اطلاعات بر آن حاکم است. اشاره‌هایی که به اقتصاد دیجیتال[1] یا موج سوم شده است، نشان‌دهنده افزایش وابستگی به فناوری اطلاعات است. با افزایش نگرانی‌ها نسبت به تهدیدهای احتمالی، دولت ایالات متحده در گزارش هیات تحقیقات ملی[2] در سال ۱۹۹۱ میلادی با عنوان «کامپیوترها در معرض خطر وابستگی شدید اقتصاد ملی» به کامپیوترها اشاره کرده است. این گزارش به نگرانی‌های موجود در زمینه‌ی وابستگی به کامپیوترها در حوزه‌ی انرژی، ارتباطات، حمل و نقل هوایی و خدمات مالی اشاره نموده است. کامپیوترها برای ذخیره اطلاعات حیاتی اعم از سوابق پزشکی و برنامه‌های کسب‌وکار و سوابق جنایی مورد استفاده قرار گرفته‌اند (Gordon et al., 2005). این

1 – Digital Economy
2 – National Research Council

وابستگی تا جایی ادامه یافته است که ایالات متحده راهبرد ملی امنیت فضای سایبری در سال ۲۰۰۳ میلادی آورده است: «تا سال ۲۰۰۳ میلادی اقتصاد و امنیت ملی ما کاملاً به زیرساخت‌های اطلاعاتی وابسته خواهد بود. شبکه‌ای از شبکه‌ها، پشتیبانی مستقیم عملیات همه‌ی بخش‌های اقتصاد، انرژی، حمل‌ونقل، مالی و بانکی، اطلاعاتی و ارتباطی، بهداشت و سلامت عمومی، خدمات اضطراری، آب، پزشکی، تأسیسات دفاعی، تغذیه، کشاورزی و حمل و نقل و پست را برعهده خواهد گرفت».

بخش خصوصی هدف اصلی جنگ‌های اطلاعاتی: حمله‌های سایبری، نخست اهداف نظامی را مدنظر داشتند. با افزایش وابستگی اقتصادی به فناوری اطلاعات، زیرساخت‌های شهری بیش از پیش به اهداف مورد نظر حملات سایبری تبدیل شده‌اند. عناوین خبری به حملاتی اشاره نموده‌اند که سایت‌ها و محصولات تجاری را مورد حمله وسیع قرار داده‌اند. در همین خصوص به‌عنوان نمونه: این حمله‌ها، کنگره ایالات متحده را بر آن داشت قوانین جدیدی برای تضمین ایمنی فضای سایبری در نظر بگیرند تا از این طریق ۱۰۳ راکتور اتمی موجود در ایالات متحده را مورد حمایت و محافظت قرار دهند (Gordon et al., 2005).

گسترش به‌کارگیری فناوری سایبری برای مدیریت ادراکات افراد: مدیریت ادراکات[1] فرآیندی است شامل مجموعه اقداماتی که برای تأثیرگذاری روی دیدگاه‌های عمومی و فرهنگ، انجام می‌شوند و در حوزه‌های سیاسی، مدنی، فرهنگی، سازمانی و نظامی کاربرد دارند. در روش‌های مدرن مدیریت ادراکات، فناوری‌های نوین و سریع نقشی کلیدی در متأثر نمودن افکار و ایده‌های افراد دارند. توسعه‌ی فناوری‌های اینترنتی و شبکه‌های جهانی، مدیریت ادراکات را به جنبه‌ای کلیدی در بسیاری از مبارزات و تعارض‌ها تبدیل کرده است. در جنگ‌های اعتقادی، ادراکات عموم مردم هدف قرار داده می‌شود (Rhem, 2005).

افزایش کاربرد فناوری سایبری در جاسوسی: در مارس سال ۲۰۰۱ ویلیام کوهن[2]، وزیر دفاع سابق ایالات متحده، اعلام نمود که رئیس سابق سرویس اطلاعاتی فرانسه تأیید کرده که این سازمان

1 - Perception management
2 - William Cohen

اقدام به گردآوری اطلاعات کلیدی شرکت‌های ایالات متحده و سایر شرکت‌هایی می‌کند که رقیب سازمان‌های فرانسوی هستند و این اطلاعات را به فرانسه ارسال می‌کند. او به چند نمونه جاسوسی فرانسوی‌ها علیه سازمان‌های ایالات متحده اشاره نمود. یکی از این موارد به سرقت اطلاعات فنی از کامپیوترهای ایالات متحده مربوط می‌شود که توسط سرویس اطلاعاتی فرانسه به یکی از شرکت‌های فرانسوی ارسال گردید. متوسط زیان ناشی از حمله یک هکر به یک کامپیوتر ۱۵۰ هزار دلار است که این هزینه در جاسوسی بسیار بیشتر است. جاسوسی ممکن است از طریق ایمیل‌های رد و بدل شده میان کارکنان یک سازمان با سازمان‌های رقیب انجام شود. نتایج یکی از مطالعات میدانی انجام شده در میان ٤٩٨ نفر از کارکنان سازمان‌های مختلف آشکار ساخت که ٤٠٪ آنها دریافت اطلاعات محرمانه در مورد سازمان‌های دیگر از طریق اینترنت را تایید کرده‌اند و این رقم از سال ۱۹۹۹ میلادی در حدود ۳٥٦٪ رشد داشته است. دستگاه قضایی ایالات متحده در سال ۲۰۰٤ میلادی اعلام کرد فعالیت‌های غیرقانونی اینترنتی زیادی را اعم از کلاهبرداری با کارت اعتباری و جاسوسی شناسایی کرده است. در این کشور، مأموران تحقیق و تفحص بیش از ۱۵۰ هزار قربانی حملات سایبری را شناسایی کردند که خسارات وارد بر آنها از مرز ۲۱۵ میلیون دلار می‌گذشت. لازم به ذکر است که با گسترش شبکه‌های داخلی سازمان‌ها و قرار دادن اطلاعات بیشتر در اختیار کارکنان و تأمین‌کنندگان، احتمال وقوع جاسوسی افزایش می‌یابد (Rhem, 2005).

افزایش کاربرد فناوری در جرایم سازمان‌یافته: انفجار اینترنتی منجر به ظهور و بروز جرایم نوینی در فضای سایبری گردید. در همین خصوص دستگاه قضایی ایالات متحده مدعی است کلاهبرداری‌های اینترنتی و سایر جرم‌های آنلاین، جزء جرایمی هستند که در حال افزایش با بالاترین نرخ هستند. یکی از روش‌های مورد استفاده این مجرمین، استفاده از سایت‌های تقلبی با ظاهری مشابه سایت اصلی است. متخصصین در زمینه ویروس‌کش‌ها فعالیت‌های بسیاری را در حوزه‌ی تولید ویروس و کرم نرم‌افزاری گزارش کرده‌اند و رشد سریع این نوع جرم را شناسایی کرده‌اند. فعالیت‌های زیرزمینی و غیر قانونی این‌چنینی در راستای تقویت اقتصاد موسوم به زیرزمینی می‌شود که تمرکز آن بر روی کلاهبرداری است (Rhem, 2005).

گسترش استفاده از فناوری سایبری بر علیه اشخاص و کسب‌وکارهای کوچک: امروزه نرم‌افزارهای موسوم به جاسوس‌افزارها[1] افراد و کسب‌وکارهای کوچک را تهدید می‌کنند. آنها برنامه‌های کاربردی معمولی هستند که مورد استفاده یا موافقت کاربران قرار می‌گیرند و عمل پایش مداوم را انجام می‌دهند. تاکنون وجود ۷۰۰۰ جاسوس افزار شناسایی شده است که بنابر گزارش شرکت مایکروسافت[2]، مسوول خرابی نیمی از کامپیوترها هستند. نتایج یک مطالعه نشان داده است ۹۱٪ کامپیوترهای خانگی تحت تأثیر جاسوس افزارها قرار دارند.

یکی دیگر از مشکلات رو به افزایش، سرقت هویت است که نوع جدیدی از تروریسم سایبری بر علیه اشخاص تلقی می‌شود که اغلب برای انجام اعمال غیرقانونی و مجرمانه با نام فردی دیگر، انجام می‌شود. چنین اقدامی هم افراد و هم کسب‌وکارها را با مشکل مواجه می‌کند. در گزارش کمیسیون تجارت فدرال[3] آمده است طی سال ۲۰۰۳ حدود ۹/۹ میلیون نفر در ایالات متحده قربانی این جرم شدند. اغلب این موارد توسط سارقان سایبری انجام شده که هویت افراد را برای بازکردن حسابی جدید سرقت می‌کردند و خسارت هریک از این موارد به طور متوسط ۱۲۰۰ دلار برآورد شده است. حساب‌های تقلبی تاکنون ۳۲/۹ میلیارد دلار خسارت به کسب‌وکارها و ۳/۸ میلیارد دلار خسارت به مصرف‌کنندگان تحمیل کرده‌اند (Rhem, 2005).

روش‌شناسی تحقیق

این پژوهش که از نوع پژوهش‌های کیفی می‌باشد، به‌دنبال پاسخ به سؤالات ذیل به انجام رسیده است که عبارتند از:

- رزم اطلاعات چیست و چه ابعادی دارد؟
- از طرفی مباحث متنوع ذکر شده در ادبیات در حوزه‌ی رزم اطلاعاتی را چگونه می‌توان در کنار هم قرار دادو مدل تحلیل آن چیست؟

1 – Spyware
2 – Microsoft Corporation
3 – Federal Trade Commission

در واقع، این پژوهش به دنبال تبیین مفاهیم، رفع ابهامات و مدیریت دیدگاه‌های گوناگون در حوزه‌ی رزم اطلاعات است. در نهایت این پژوهش سعی دارد تا به جای بررسی عوامل تأثیرگذار بر (و یا مؤثر از) رزم اطلاعات، به تبیین و تشریح ماهیت درونی و چیستی رزم اطلاعات بپردازد.

سؤالی که از منظر روش شناسی مطرح می‌شود آن است که چه نوع خروجی نظری می‌تواند قالب مناسبی برای پاسخ ارائه شده این پژوهش به سؤالات آن باشد. به عبارتی باید تعیین نمود که کدام یک از انواع خروجی‌های نظری و یا ترکیبی از آنها مانند مدل‌ها، روش‌ها، سازه‌ها، چارچوب‌ها می‌تواند بهترین گزینه برای خروجی پژوهش حاضر باشد. برای پاسخ به این سوال بایستی به گونه‌شناسی[1] نظریه‌ها پرداخت. یکی از بهترین تحقیقات در این زمینه، توسط شرلی گرگور[2] به انجام رسیده است. گرگور پنج نوع نظریه در حوزه فناوری اطلاعات را شناسایی نموده است که به شرح جدول شماره‌ی (۲) می‌باشد.

جدول شماره‌ی ۲ – انواع نظریه‌های حوزه فناوری اطلاعات (Gregor, 2006)

نوع نظریه	ویژگی‌های نظریه
نظریه برای تحلیل	به سؤال «چه چیزی» پاسخ می‌گوید. هیچ روابط علی بین پدیده‌ها و متغیرها در این نوع نظریه مطرح نمی‌شود و هیچ‌گونه پیش‌بینی صورت نمی‌گیرد.
نظریه برای تبیین	به سؤال «چه چیزی، چگونه، چرا، چه زمانی و کجا» پاسخ می‌گوید. این نوع نظریه به تبیین پدیده‌ها می‌پردازد اما به دنبال پیش‌بینی نیست. هیچ فرضیه آزمون‌پذیری ارائه نمی‌گردد.
نظریه برای پیش‌بینی	به سؤال «چه چیزی است و چه خواهد بود» پاسخ می‌گوید. این نوع نظریه به ارائه پیش‌بینی پرداخته و شامل فرضیات آزمون‌پذیر می‌باشد.
نظریه برای تبیین و پیش‌بینی	به سؤال «چه چیزی، چگونه، چرا، چه زمانی، کجا و چه خواهد بود» پاسخ می‌گوید. این نوع نظریه به ارائه پیش‌بینی می‌پردازد و هم شامل فرضیات آزمون‌پذیر و هم روابط علی می‌باشد.
نظریه برای طراحی و اجرا	به سؤال «چگونه کاری را انجام دهیم» پاسخ می‌گوید. این نظریه تجویزات صریحی (مانند روش‌ها و تکنیک‌ها) را برای ساخت مصنوعات ارائه می‌نماید.

1 – Ontology
2 – Shirley Gregor

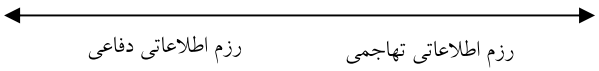
هر یک از انواع نظریه‌های فوق‌الذکر در قالب‌های گوناگونی ارائه می‌شوند که گرگور به قالب‌های معمول اشاره نموده است. وی معتقد است «نظریه برای تحلیل» غالباً به‌صورت طبقه‌بندی‌ها و چارچوب‌ها ارائه می‌شوند. به عقیده گرگور، این نوع نظریه بیشتر در مواقعی کاربرد دارد که شناخت و درک نسبتاً کمی درباره پدیده‌ی تحت بررسی وجود داشته و چیستی پدیده‌ی مورد نظر به‌خوبی تبیین نشده است (Gregor, 2009). از آنجا که پژوهش حاضر نیز به دنبال مفهوم‌سازی رزم اطلاعاتی و تبیین چیستی آن است، از این رو این پژوهش بایستی به ارائه چارچوبی برای این منظور بپردازد.

به‌طور کلی چارچوب عبارتند از یک ساختار مفهومی بنیادین که برای بررسی و حل مسائل پیچیده مورد استفاده استقرار می‌گیرد. چارچوب‌ها یک ساختار زیربنایی برای پشتیبانی از چیزی و یا دربر گرفتن برخی مفاهیم مرتبط به هم فراهم می‌نمایند. چارچوب‌های مربوط به حوزه‌ی فناوری اطلاعات و کاربردهای آن در بخش‌های گوناگون، به درک حوزه‌ها و ابعاد مختلف آنها کمک می‌نماید و از این رو، از دیدگاه مفهومی، چارچوب‌ها به پیچیدگی حوزه‌های مرتبط با فناوری اطلاعات نظم بخشیده و منجر به مدیریت بهتر پیچیدگی‌های درونی این حوزه‌ها می‌شوند. چارچوب‌های یک حوزه، تعیین کننده دستگاه مفهمومی است که هنگام فعالیت در یک حوزه به کار می‌بریم و یا بر آن دستگاه مفهومی تأثیرگذار است (Basden, 2008). این چارچوب‌ها تعیین می‌کنند که چگونه پدیده‌ها را طبقه بندی می‌کنیم، چه نظریه‌هایی را اتخاذ می‌نماییم و چه نوع متدلوژی‌ها و قوانینی را برای هدایت تحقیق و یا پژوهش فرموله می‌کنیم، چه موارد و موضوعات با اهمیتی را در آن حوزه تشخیص می‌دهیم، چه سؤالاتی از خودمان خواهیم پرسید، چه مواردی را به عنوان مشکلات و چه راه‌حل‌هایی برای حل این مشکلات بر می‌گزینیم. درستی یا نادرستی یک چارچوب به‌وسیله‌ی مفاهیم نظری قابل اثبات نیست. چرا که یک چارچوب به عنوان یک پیش‌نظریه از مجموعه‌ای از باورها و مفروضات درباره حوزه‌ای که به‌وسیله کسانی که در آن حوزه کار می‌کنند شکل گرفته است (Basden, 2008).

چارچوب رزم اطلاعاتی

چارچوبی که برای رزم اطلاعاتی در این مقاله ارائه گردیده است بر سه محور بنا نهاده شده است. اولین محور بر «جهت رزم اطلاعاتی» اشاره دارد، این محور شامل دو بعد است (شکل شماره‌ی ۱ را ببینید):

- رزم اطلاعاتی دفاعی: رزم اطلاعاتی دفاعی زمانی رخ می‌دهد که رزم اطلاعاتی با هدف دفاع از سیستم‌ها و سرمایه‌های اطلاعاتی صورت می‌پذیرد. این امر ممکن است از طریق عملیات فیزیکی و یا عملیات نرم افزاری و سایبری و سایر شیوه‌های دفاعی صورت پذیرد.
- رزم اطلاعاتی تهاجمی: در رزم اطلاعاتی تهاجمی، سیستم‌ها و سرمایه‌های اطلاعاتی دشمن از طریق عملیات فیزیکی و یا عملیات نرم‌افزاری و سایبری و سایر شیوه‌های رزم، مورد تهاجم و تخریب قرار می‌گیرد.



شکل شماره‌ی ۱ - ابعاد محور «جهت رزم اطلاعاتی»

دومین محور چارچوب، بر «عمق رزم اطلاعاتی» تأکید دارد. این محور دارای دو بعد می‌باشد (شکل شماره‌ی ۲ را ببینید):

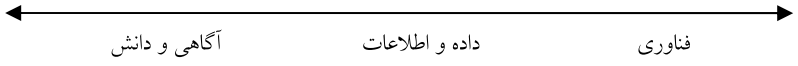
- رزم‌های اطلاعاتی راهبردی: در برخی از رزم‌های اطلاعاتی، با بهره‌گیری از ابزارها و روش‌های حاصل از انقلاب اطلاعاتی، دارایی‌های راهبردی کلیدی کشورها اعم از زیرساخت‌های بخش‌های انرژی، ارتباطات، حمل‌ونقل، مالی تهدید می‌گردد.
- رزم‌های اطلاعاتی معمول: در این‌گونه رزم‌های اطلاعاتی، هدف‌های رزم اطلاعاتی جنبه راهبردی ندارد.

شکل شماره‌ی ۲ - ابعاد محور «عمق رزم اطلاعاتی»

سومین محور بر «عناصر رزم اطلاعاتی» تأکید دارد. همان‌طور که در پیش‌تر ذکر شد، ظهور و به‌کارگیری فناوری‌های اطلاعاتی در حوزه‌ی دفاعی عاملی بنیادی در راستای شکل‌گیری مفهوم رزم اطلاعاتی بوده است. به‌عبارتی، یکی از ریشه‌های رزم اطلاعاتی را بایستی در فناوری اطلاعات جستجو کرد. بررسی ادبیات نشان می‌دهد که مباحث حوزه‌ی رزم اطلاعاتی با تأکید بر عناصر و اجزای مختلف فناوری‌های اطلاعاتی، به تبیین مفهوم رزم اطلاعاتی و تشریح آن پرداخته‌اند.

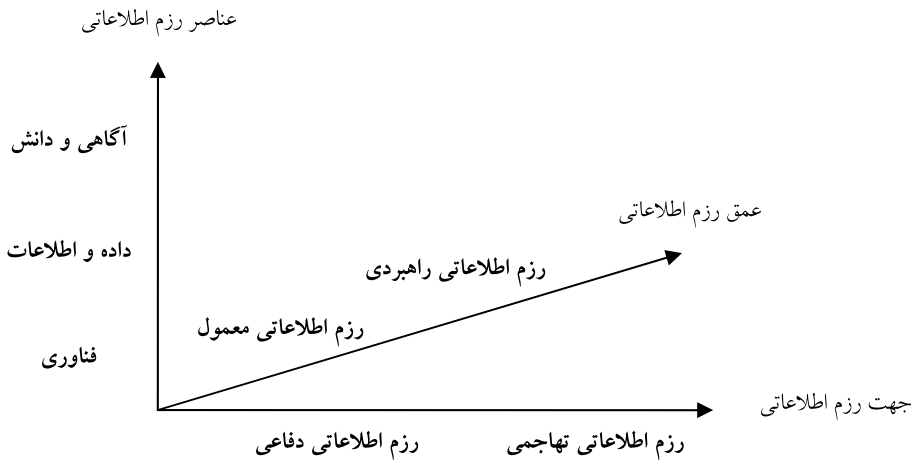
ادبیات مربوطه را می‌توان در دو بخش عمده تقسیم بندی نمود (شکل شماره‌ی ۳ را ببینید):

- تأکید بر اطلاعات: دسته اول بر اطلاعات تأکید دارند. منظور از تأکید بر اطلاعات در رزم اطلاعاتی آن است که رزم چه در حالت دفاع و چه در حالت تهاجم با تکیه بر قابلیت‌های اطلاعاتی به انجام می‌رسد. در رویکرد رزم اطلاعاتی دفاعی، از قابلیت‌های اطلاعاتی برای دفاع در برابر شیوه‌های گوناگون حمله، بهره گرفته می‌شود. در رویکرد رزم اطلاعاتی تهاجمی، از قابلیت‌های اطلاعاتی برای حمله همه‌جانبه به دشمن استفاده می‌شود. تأکید بر اطلاعات نیز به نوبه‌ی خود در دو شاخه قابل بررسی است. برخی از ادبیات بر سطوح انتزاع بالای اطلاعات که شامل آگاهی و دانش می‌باشد تأکید داشته و برخی نیز بر سطوح انتزاع پائین‌تر اطلاعات که شامل داده و اطلاعات (در معنای عام) است، تمرکز داشته‌اند.
- تأکید بر فناوری: دسته دوم بر فناوری تأکید دارند که در رزم‌های اطلاعاتی مبتنی بر فناوری، در رویکرد دفاعی، از قابلیت‌های فناوری (که پشتیبانی کننده عملیات مربوط به جمع‌آوری، پردازش، ذخیره و انتشار اطلاعات است) برای مقابله با شیوه‌های گوناگون حمله، بهره گرفته می‌شود و در رزم‌های اطلاعاتی مبتنی بر فناوری، در رویکرد تهاجمی نیز از قابلیت‌های فناوری برای حمله همه‌جانبه به دشمن استفاده می‌شود.



شکل شماره‌ی ۳ - ابعاد محور «عناصر رزم اطلاعاتی»

محورهای تشکیل‌دهنده‌ی چارچوب رزم اطلاعاتی در شکل شماره‌ی ٤ نشان داده شده است.



شکل شماره‌ی ٤ – محورهای تشکیل‌دهنده‌ی چارچوب رزم اطلاعاتی

به‌منظور تشریح محورهای چارچوب رزم اطلاعاتی، محورهای نشان داده شده در شکل شماره‌ی ٤، در قالب ماتریس دوبعدی (جدول شماره‌ی ۳) ارائه گردیده است. این ماتریس نشان‌دهنده‌ی چارچوب رزم اطلاعاتی می‌باشد.

جدول شماره‌ی۳ – چارچوب رزم اطلاعاتی

			جهت رزم اطلاعاتی	
		عمق رزم اطلاعاتی	رزم اطلاعاتی دفاعی	رزم اطلاعاتی تهاجمی
عناصر رزم اطلاعات	آگاهی و دانش	رزم اطلاعاتی معمول	۱. رزم اطلاعاتی دفاعی مبتنی بر آگاهی و دانش	۲. رزم اطلاعاتی تهاجمی مبتنی بر آگاهی و دانش
		رزم اطلاعاتی راهبردی	۳. رزم اطلاعاتی راهبردی دفاعی مبتنی بر آگاهی و دانش	٤. رزم اطلاعاتی راهبردی تهاجمی مبتنی بر آگاهی و دانش
	داده و اطلاعات	رزم اطلاعاتی معمول	٥. رزم اطلاعاتی دفاعی مبتنی بر داده و اطلاعات	٦. رزم اطلاعاتی تهاجمی مبتنی بر داده و اطلاعات
		رزم اطلاعاتی راهبردی	۷. رزم اطلاعاتی راهبردی دفاعی مبتنی بر داده و اطلاعات	۸. رزم اطلاعاتی راهبردی تهاجمی مبتنی بر داده و اطلاعات

ادامه‌ی جدول شماره‌ی ۳			
فناوری	رزم اطلاعاتی معمول	۹. رزم اطلاعاتی دفاعی مبتنی بر فناوری	۱۰. رزم اطلاعاتی تهاجمی مبتنی بر فناوری
	رزم اطلاعاتی راهبردی	۱۱. رزم اطلاعاتی راهبردی دفاعی مبتنی بر فناوری	۱۲. رزم اطلاعاتی راهبردی تهاجمی مبتنی بر فناوری

چارچوب فوق آنچه را که در ادبیات رزم اطلاعاتی مطرح شده است، در خود جای می‌دهد. مباحثی نظیر رزم مبتنی بر شبکه، رزم مبتنی بر دانش، رزم اطلاعاتی راهبردی و رزم سایبری اصطلاحاتی هستند که تحت عنوان رزم اطلاعاتی در ادبیات ذکر شده‌اند و هر یک بر بعدی خاص از رزم اطلاعاتی اشاره دارند. چارچوب ارائه شده با مورد توجه قرار دادن ابعاد زیر بنایی رزم اطلاعاتی، مبنایی را برای تبیین جایگاه هر یک از اصطلاحات و برداشت‌ها از رزم اطلاعاتی و تبیین تمایزات بین آنها فراهم نموده است.

در بخش بعد برخی از این اصطلاحات و ادبیات مربوطه بر سلول‌های مختلف چارچوب پیشنهادی نگاشت می‌شود. بررسی‌ها نشان می‌دهد که در ادبیات موجود رزم اطلاعاتی، ادبیات حوزه‌ی رزم اطلاعاتی مبتنی بر آگاهی و دانش و نیز رزم اطلاعاتی مبتنی بر فناوری بیشتر جنبه تهاجمی و ادبیات حوزه‌ی رزم اطلاعاتی مبتنی بر داده و اطلاعات بیشتر جنبه دفاعی دارد. پیشنهاد می‌شود در پژوهش‌های آتی به تبیین محتوای سایر سلول‌های چارچوب بر اساس ادبیات پرداخته شود. چه بسا این امر منجر به شکل‌گیری مفاهیم و روش‌های نوینی در رزم اطلاعاتی گردد.

کاربرد نظری چارچوب پیشنهادی در فضای رزم

در این بخش سه مفهوم پر کاربرد در حوزه رزم اطلاعاتی به سلول‌های مربوطه در چارچوب رزم اطلاعاتی اختصاص یافته و تشریح گردیده است. این مفاهیم عبارتند از: رزم دانش‌محور[1]، رزم اطلاعاتی راهبردی[2]، رزم مبتنی بر شبکه[3]. رزم دانش‌محور یکی از گونه‌های

1 – Knowledge-based Warfare (KBW)
2 – Strategic Information Warfare (SIW)
3 – Net-Centric Warfare

رزم اطلاعاتی مبتنی بر آگـاهی و دانـش اسـت کـه در ایـن بخـش از رویکـرد رزم اطلاعـاتی تهاجمی مورد بررسی قرار می‌گیرد. رزم اطلاعاتی راهبردی در طبقه‌ی راهبـردی از رزم مبتنـی بر آگاهی و دانش قرار دارد که در این بخش از رویکرد تهاجمی بررسی می‌شود. رزم مبتنی بر شبکه نیز در گروه رزم اطلاعاتی مبتنی بر فناوری قرار می‌گیرد که از دیـدگاه تهـاجمی و غیـر راهبردی مورد بررسی قرار می‌گیرد.

رزم دانش محور: رزم اطلاعاتی تهاجمی مبتنی بر آگاهی و دانش (سلول ۲)

با پیشرفت فناوری اطلاعات، مباحثی در زمینه نحـوه‌ی بـه‌کـارگیری قابلیـت‌هـای آن در تغییرات سازمانی و فرآیندی و ایجاد زیرساخت دگرگونی جنگ‌ها، موسـوم بـه انقـلاب امـور نظامی[1]، طرح گردید. به‌واقع، در صورت تلفیق فنـاوری اطلاعـات و فرآینـدهـا بـا عملیـات و مفاهیم جدید سازمانی، فرصت‌هایی برای تغییرات غیرمسـتمر و حرکـت از عصـر صـنعتی بـه عصر اطلاعاتی فراهم می‌شود. مشکل امنیت را می‌توان در کوتاه‌مـدت بـه کمـک فرآینـدهـا و فناوری عصر اطلاعات و در نهایت از طریق شکل‌دهی نیروهایی حل نمود. اما دستیابی به ایـن هدف، مستلزم برخورداری از چشم‌انداز راهبردی مشترک دولت و صنایع، به‌ویـژه بخـش‌هـای خدماتی است. لازم است بخش‌های خدماتی، فلسـفه و دیـدگاه‌هـای مشـترکی را در حـوزه‌ی مبارزه و نبرد توسعه دهند که مبنای تغییرات سازمانی و فرآیندی مورد نیاز برای توانمند و کارا نمودن نیروها قرار گیرند. همچنین لازم است این مفهوم، زیربنای سـرمایه‌گـذاری خـدمات در تحقیق، توسعه و اکتساب تلقی شود. بدین ترتیب زیربنایی منسجم و همسان برای برنامه‌ریـزی هزینه‌های دفاعی و اقدامات توسعه و خرید ایجاد می‌شود. چنین چشم‌اندازی، رزم دانش‌محور نامیده می‌شود (Casper and Halter, 1996).

رزم دانش‌محور انقلابی منطقی است از راهبردهای تهدیدمحور عصر صنعت به راهبـردهـای مبتنی بر قابلیت‌ها در عصر اطلاعات. رزم دانش‌محور، فرآیندی است که برتری آگاهی نیـروهـا در میدان جنگ را تضمین می‌کند و امکان اتخاذ سریع‌تر تصمیمات، در مقایسـه بـا دشـمن، را فـراهم

1 - Revolution in military affairs (RMA)

می‌کند. این نوع رزم، موجب کسب برتری اطلاعـاتی در جنـگ و توفیـق در رسـیدن بـه اهـداف، به‌واسطه‌ی استفاده دقیق و درست از قدرت و توان نظامی می‌شود. تفاوت رزم دانش‌محور با انـواع دیگر رزم، هم‌افزایی ابزارهای مختلف اعم از حسگرهای پیشـرفته، فنـاوری اطلاعـات و ابزارهـای تحلیلی پردازشگر اطلاعات است؛ که اطلاعات متنوعی را در مورد میدان نبرد در اختیار فرمانـدهان قرار می‌دهد و آنها خواهند توانست به کمک این اطلاعات، از تجربه‌ی نظـامی و قـدرت قضـاوت خود حداکثر استفاده را بکنند. توانایی گردآوری اطلاعات، تحلیل و پردازش و بهره‌گیـری از آن در فضای نبرد، همان برتری اطلاعاتی است. فرمانـدهان و تصـمیم‌گیرنـدگان همـواره در جسـتجوی اطلاعاتی بوده‌اند که بتوانند سرعت و قدرت عمل خود را بیشتر نموده و پیوسـته بـرای مقابلـه بـا دشمنان خود آماده باشند. امروزه، این کار امکان‌پذیر شده است. برخـورداری از مزیـت اطلاعـاتی می‌تواند به چرخه تصمیم‌گیری دشمن، ضربه سنگینی وارد کنـد. فرمانـدهان مـی‌تواننـد از طریـق کانال‌های ارتباطی به اهداف مورد نظر خود دست یابند و از نبردهای سـنگین و خسـارت‌هـای آن حتی‌الامکان اجتناب کنند. این راهبرد، موجب تقویـت برتـری اطلاعـاتی و کسـب مزیـت پایـدار راهبردی می‌شود (Lambe, 2003).

رزم دانش‌محور، به گردآوری و تحلیل اطلاعات وابسـته اسـت. یـک سیسـتم یکپارچـه فرماندهی، کنترل، محاسبه، اطلاعات عملیات، دیده‌بانی و شناسایی، به انجام یک برنامـه‌ریـزی پویا و پشتیبانی از تصمیم‌گیری‌هـا و برنامـه‌هـا کمـک مـی‌کنـد. چنـد نکتـه‌ی جدیـد در رزم دانش‌محور وجود دارد. در رزم دانش‌محـور، اولویـت بـا توسـعه‌ی سیسـتم‌هـای یکپارچـه‌ی فرماندهی و کنترل است و پس از آن به سیستم‌های مسلح طراحی شده برای کار در چارچوب فرماندهی و کنترل پرداخته می‌شود. این امر منجر به تغییر روند تولیـد سـلاح‌هـای پیشـرفته و اتکای آن به نیازهای فرماندهی و کنترل می‌شـود. در رزم دانـش‌محـور بـه‌جـای تـلاش بـرای فرسایش نیروهای دشمن در نبردی خطی، به تخریب فیزیکی اهداف مورد نظـر بـا رویکـردی غیرخطی، در داخل و خارج میدان نبرد توجه می‌شود. بنابراین، فرآیندی ترسـیم مـی‌شـود کـه تعیین‌کننده و پیش‌بینی‌کننده تأثیر اقدامات و سیستم‌های دشمن و میـزان تـأثیرات مرگبـار آنهـا است (Connery, 2003).

شبکه‌ها، اطلاعاتی را منتشر می‌کنند که می‌توانند با کمک به تصمیم‌گیری‌های افراد، آنها را در سطوح راهبردی، عملیاتی و تاکتیکی توانمند نمایند. سربازان، در صورتی که از برتری آگاهی و دانش کافی در مورد اهداف مورد نظر برخوردار باشند، می‌توانند خروجی‌های راهبردی مورد نظر را محقق نمایند. اطلاعات کاربردی در فرآیند تصمیم‌گیری منجر به افزایش سرعت ایجاد فرصت، اتخاذ تصمیمات در مورد خط مشی مبارزه، تسریع برنامه‌ریزی و پیاده‌سازی آن، و تطبیق سریع با فرآیندهای امنیتی می‌شود. تطبیق به‌موقع، نتیجه منطقی فرآیند پایش همزمان، ارائه بازخورد و تحلیل معیارهاست که نتیجه‌ی آن تسریع کل فرآیندهای امنیتی از نقطه پایش پیش از بحران تا اجرای تصمیمات اتخاذ شده برای رفع بحران را شامل می‌شود (Lambe, 2003).

در رزم دانش‌محور بر کنترل سرعت مبارزه تأکید می‌شود که نتیجه‌ی آن ایجاد برتری اطلاعاتی فرماندهان در مورد زمان، مکان و تحرکات مورد نظر آنها است. در این صورت زمان به یکی از معیارهای اثربخشی فرآیندهای امنیتی تبدیل می‌شود که جنگ‌های موازی، نقطه غایی چنین رویکردی است. ترکیب دانش میدان جنگ با توانایی حمله‌ی دقیق و هم‌راستا با اهداف کلیدی، با سرعت و کشندگی زیاد، قابلیت‌های چشمگیری را برای به زانو درآوردن سریع یک ارتش یا جامعه‌ی پیشرفته و صنعتی در اختیار قرار می‌دهد. به واقع رزم دانش‌محور، دیدگاه‌های ذهنی جدیدی در مورد برنامه‌ریزی و اشتراک اطلاعات دارد.

این رویکرد، از برنامه‌ریزی پویا، تعاملی و هماهنگ استقبال می‌کند و بر هدف‌گیری سیستماتیک و نتیجه‌محور اهداف و نتایج راهبردی مورد انتظار، تأکید دارد. توزیع موازی اطلاعات میان رده‌های مختلف اعم از سربازان تا تصمیم‌گیران و بهره‌گیری از عامل‌های هوشمند برای مرتب نمودن اطلاعات قابل‌استفاده در تصمیم‌گیری، از ویژگی‌های دیگر آن است. تأکید اصلی آن روی تحلیل داده، ایجاد اطلاعات قابل استفاده در تصمیم‌گیری و در نهایت دانش است. رزم دانش‌محور فرصت‌هایی را فراهم می‌کند که اثرات چشمگیری بر راهبرد امنیت ملی دارند؛ نه تنها قابلیت‌های آن را بهبود می‌بخشند، بلکه موجب افزایش گزینه‌های تصمیم‌گیرانی می‌شود که از دانش تولید شده در یک حوزه مشترک بهره می‌گیرند و

با اقدامات سیاسی، دیپلماتیک و نظامی خود می‌کوشند مانع از بروز جنگ و درگیری شوند. آنها می‌توانند با تسهیل دوران گذار به سوی نیروهای کارآمدتر و توانمندتر، از بروز تعارضات عظیم و وسیع پیشگیری کرده و ابزاری را در اختیار تدوین‌کنندگان خط‌مشی قرار دهند تا بتوانند در آینده محیط امنی را فراهم نمایند (Evans, 2012).

رزم اطلاعاتی راهبردی: رزم اطلاعاتی راهبردی تهاجمی مبتنی بر داده و اطلاعات (سلول ۸)

این احتمال وجود دارد که در آینده نیروهای نظامی با بهره‌گیری از ابزارها و روش‌های حاصل از انقلاب اطلاعاتی، دارایی‌های راهبردی کلیدی ملت‌ها اعم از زیرساخت‌های بخش‌های انرژی، ارتباطات، حمل‌ونقل، مالی و... دشمنان خود را تهدید نمایند. این خطر بالقوه، از ویژگی‌های ماهوی محیط رزم اطلاعاتی راهبردی به شمار می‌رود. دشمنان و رقبای اقتصادی ممکن است از ابزارها و تکنیک‌های رزم اطلاعاتی راهبردی برای به چالش کشیدن کشورها، منافع و متحدان آنها، بهره‌گیری نمایند. در آینده‌ی نزدیک سلاح‌های رزم اطلاعاتی راهبردی می‌توانند مورد استفاده دشمنان باشند که در صورت ضعف در مقابله فیزیکی، به استفاده از راهبردهای نامتقارن[1] روی می‌آورند. این راهبرد ترکیب ابزارهای رزم اطلاعاتی راهبردی با سلاح‌های هسته‌ای، شیمیایی، بیولوژیک و جنگ‌افزارهای معمولی را می‌طلبند (Molander et al., 1996).

در رزم اطلاعاتی راهبردی، میدان نبرد همان زیرساخت اطلاعاتی جوامع مدرن است که وابستگی جامعه به آن در سیستم‌های تأمین انرژی، مالی، کنترل ترافیک و سایر سیستم‌های کامپیوتری نمود پیدا می‌کند. رزم اطلاعاتی راهبردی برخاسته از اینترنت است و در آن از اینترنت استفاده زیادی می‌شود. ارتباط تعداد زیادی از کامپیوترها با یکدیگر، آنها را مستعد آسیب‌پذیری در مقابل وقفه‌ها و ضعف‌های سیستماتیک می‌کند. این امکان وجود دارد از خارج از کشور حمله‌هایی به کامپیوترها شود که ردیابی آنها امکان‌پذیر نباشد. در اکثر موارد این کار به قدری زیرکانه و ماهرانه صورت می‌گیرد که تا پایان حمله، کسی متوجه آن نمی‌شود

1 - Asymmetric Strategies

و بعد از اتمام آن دیگر دیر شده و فرصتی برای مقابله وجود ندارد. ایالات متحده اصولاً آسیب‌پذیری خاصی در مقابل چنین حمله‌هایی دارد، چرا که از پیشرفته‌ترین سیستم‌های کامپیوتر برخوردار است و وابستگی نسبی بیشتری به آنها دارد (Molander et al., 1996).

با وجود این‌که زیرساخت‌های اطلاعاتی مورد نیاز برای رزم راهبردی اطلاعاتی به اینترنت محدود نمی‌شوند، شبکه‌ها به‌قدری با اینترنت عجین شده‌اند که این دو، یک موجودیت به نظر می‌رسند. در نتیجه، خطرات و نقاط ضعف اینترنت، جدی‌ترین تهدیدها برای زیرساخت‌های اطلاعاتی به شمار می‌روند. گزارش‌های منتشر شده در مورد حمله‌های کامپیوتری، جرائم الکترونیک و تروریسم اطلاعاتی، باعث شده این تصور در عموم مردم حاکم شود که اتصال به شبکه و دسترسی از راه دور، فقدان سیستم کنترل‌کننده مرکزی و ارتباطات متقابل و چند جانبه موجب شده اینترنت و به طور کلی کامپیوترها فاقد امنیت باشند. بسیاری از این گزارش‌ها غلط و احساسی هستند، اما ضعف دانش فنی عمومی نسبت به کامپیوترها و شبکه مرتباً به شایعات و نگرانی‌ها دامن می‌زند (Molander et al., 1998).

در تاریخ رزم‌های راهبردی، یافتن نبردی که در آن از اطلاعات مهم و حساس به‌عنوان یکی از حربه‌های اصلی مبارزه استفاده نشده باشد، مشکل است. در همین راستا، سان تزو استفاده از اطلاعات را برای دستیابی به اهداف راهبردی، به موازات اجتناب از تعارض فیزیکی پیشنهاد می‌کند. بدون شک می‌توان فهرستی از وقایع تاریخی تهیه نمود که در آنها تغییرات بنیادین فناوری منجر به تغییر نقش و جایگاه اطلاعات در نبردهای راهبردی شده است.

هنوز تأثیر بالقوه انقلاب اطلاعات روی رزم‌های راهبردی به‌خوبی روشن نیست. رزم اطلاعاتی راهبردی در گذشته نقش زیرمجموعه را در رزم‌های راهبردی ایفا نموده است، در حالی که ممکن است در اوج انقلاب اطلاعاتی نقشی بسیار مهم‌تر را ایفا کند. تأثیر بالقوه انقلاب اطلاعات روی آسیب‌پذیری زیرساخت‌های ملی و سایر دارایی‌های راهبردی ممکن است در گذر زمان تغییر کرده و منجر به بروز نوع کاملاً جدیدی از رزم‌های راهبردی مبتنی بر اطلاعات شود. به‌طور کلی می‌توان دو نسل را برای رزم اطلاعاتی راهبردی متصور شد (Molander et al., 1998).

۱) رزم اطلاعاتی راهبردی نسل اول: رزم اطلاعاتی راهبردی به‌عنوان یکی از اشکال یا اجزای رزم‌های راهبردی در آینده است، که مفهوم آن حرکت به جلو از طریق هماهنگی تعدادی از ابزارهای مختلف رزم راهبردی می‌باشد.

۲) رزم اطلاعاتی راهبردی نسل دوم: رزم اطلاعاتی راهبردی به‌عنوان نوعی مستقل و جدید از رزم راهبردی شناخته می‌شود که در نتیجه‌ی انقلاب اطلاعاتی ظهور کرد. در حیطه‌های نوظهوری از رزم راهبردی (مانند اقتصاد) و در طول زمان (مثلاً سال در مقابل روز، هفته و ماه) کاربرد دارد و زمان مورد نیاز برای آن عموماً طولانی‌تر از رزم‌های راهبردی است.

صاحب‌نظران بر این باورند که ابر قدرت‌ها و قدرت‌های نوظهور منطقه‌ای، به احتمال زیاد از رزم اطلاعاتی راهبردی نسل اول بهره خواهند گرفت. البته این دیدگاه قابل بحث و بررسی است. برای مثال ممکن است قدرت‌های برتر در آینده نزدیک با شرایطی مواجه شود که ترجیح دهد از مزیت‌های فناوری اطلاعات خود بهره‌برداری نموده و رزم اطلاعاتی راهبردی نسل دوم را به‌کار گیرد تا از بروز شرایطی که در نهایت منجر به نبرد فیزیکی وسیع و خسارات فراوان می‌شود، پیشگیری کند (Molander et al., 1998).

رزم اطلاعاتی مبتنی بر شبکه: رزم اطلاعاتی تهاجمی مبتنی بر فناوری (سلول ۱۲)

با ورود به هزاره سوم، مسائل نظامی پا به عرصه جدیدی گذاشته‌اند؛ دورانی که در آن رزم متأثر از محیط متغیر راهبردی و تغییرات سریع فناوری است. کشورهای مختلف در حال تجربه گذار از عصر صنعتی به عصر اطلاعاتی هستند. این تغییرات، به موازات تجربه‌های کسب شده در عملیات نظامی گذشته، موجب ظهور رویکرد جدیدی شده که جنگ مبتنی بر شبکه[1] و عملیات مبتنی بر شبکه‌ی هسته مرکزی آن را تشکیل می‌دهد. برای درک بهتر، اهمیت تجهیز نیروهای مسلح به ابزارهای جنگ مبتنی بر شبکه، بایستی به سؤالات اساسی مطرح در زمینه‌ی ظهور رزم مبتنی بر شبکه به‌عنوان یک نظریه‌ی نظامی در عصر اطلاعات پاسخ گفت.

1 - Network-Centric Warfare

همچنین تشریح می‌شود چگونه اصول در توسعه مفاهیم، سازمان‌ها و فرآیندهای جدید جنگی کاربرد پیدا می‌کند که تأمین‌کننده مزیت رقابتی نیروهای نظامی در مقابل دشمنان احتمالی فعلی و آتی است (Office of Force Transformation, 2003).

رزم مبتنی بر شبکه، نظریه نوظهوری است که در عصر اطلاعات شکل گرفت. واژه‌ی رزم مبتنی بر شبکه، ترکیبی از راهبرد، تاکتیک‌های نوظهور، سازمان، تکنیک‌ها و رویه‌هایی است که نیروهای مجهز به شبکه می‌توانند از آن به طور کلی یا بخشی در جهت تقویت مزیت دفاعی خود بهره‌گیری کنند. نخستین عاملی که باید در پیاده‌سازی رزم مبتنی بر شبکه مورد توجه قرار گیرد، رفتار انسان‌ها در مواجهه با فناوری اطلاعات است. لذا هنگام ارزیابی میزان بهره‌برداری یک واحد یا بخش یا سازمان نظامی از رزم مبتنی بر شبکه، بر رفتار انسان‌ها در محیط شبکه‌ای تمرکز می‌شود. نیروهای نظامی در چنین فضایی چگونه رفتار می‌کنند، چه عملکردی دارند و چطور سازماندهی می‌شوند؟ تجربه نشان داده تجهیز سربازان، ملوانان، خلبانان، تفنگداران دریایی و سایر نیروهای رده‌های تاکتیکی و عملیاتی به ابزارهای مبتنی بر شبکه، موجب افزایش میزان آگاهی آنها از وضعیت و شرایط موجود شده و در مقابل دشمن مزیتی چشمگیر به آنها می‌دهد. نظریه‌ی رزم مبتنی بر شبکه قابل تعمیم و کاربرد در هر سه رده راهبردی، عملیاتی و تاکتیکی نبردها می‌باشد (Edward and Smith, 2002).

دیدگاه رزم مبتنی بر شبکه نه تنها ماهیت سازمان‌ها را متحول ساخته، بلکه عملکرد نیروهای نظامی را نیز تغییر داده و خواهد داد. به موازات توسعه‌ی زیربنای اطلاعاتی رزم مبتنی بر شبکه در عصر اطلاعات، وزارت دفاع ایالات متحده در قالب برنامه تحقیقاتی کنترل و فرماندهی مجموعه کتبی را منتشر نموده است. در اولین کتاب این مجموعه با عنوان رزم مبتنی بر شبکه: توسعه و تقویت برتری اطلاعاتی، مطالبی در زمینه‌ی ارتباط قدرت نظامی با شبکه‌های پایدار، تشریح و مکتوب شده است. در این کتاب، تأثیر و کارکرد اطلاعات در فرماندهی و کنترل و نتیجه آن در تغییر ساختارهای نظامی، تشریح شده است. در این مجموعه سه جلدی، دو عنوان دیگر نیز وجود دارد: درک مفهوم رزم در عصر اطلاعات، و تحولات عصر اطلاعات. برنامه تحقیقاتی کنترل و فرماندهی همچنین اقدام به انتشار کتاب کاربرد رزم مبتنی بر شبکه در زمان صلح، جنگ و بحران

نموده است که در آن به ارتباط متقابل میان سازمان‌ها، فرآیندها و ماموریت‌های مبتنی بر شبکه پرداخته شده است (US Office of the force transformation, 2010).

برای اجرای عملیات نتیجه‌محور[1]، برخورداری از نیروهای مجهز به ابزارهای شبکه‌محور که قابلیت اجرای عملیات مبتنی بر شبکه را دارا باشند، ضروری است. عملیات نتیجه‌محور به مجموعه اقداماتی اطلاق می‌شود که برای شکل‌دهی و هدایت رفتار حامیان، بی‌طرفان و دشمنان، در شرایط صلح، جنگ یا بحران، انجام می‌شوند. عملیات نتیجه‌محور نوع جدیدی از مبارزه به شمار نمی‌رود و تصمیم‌گیرندگان همواره در طول تاریخ به دنبال ایجاد شرایط و وضعیتی بوده‌اند که دستیابی آنها به اهداف موردنظرشان را امکان‌پذیر نماید. فرماندهان و برنامه‌ریزان نظامی همواره کوشیده‌اند با طرح‌ریزی سلسه اقدامات و مبارزات، چنین شرایطی را به‌وجود آورند که این اقدام در ادبیات نظامی امروزی، عملیات نتیجه‌محور نامیده می‌شود. این مفهوم که در قرن ۲۱ توسط نیروهای مجهز به شبکه توسعه‌یافته، به متدلوژی برنامه‌ریزی، پیاده‌سازی و اجرا، و ارزیابی عملیات نظامی اشاره دارد که با هدف به‌جا گذاشتن تأثیری خاص انجام می‌شود که منجر به حصول نتایج مورد نظر در حوزه‌ی امنیت ملی می‌شود. نیروهای مسلح ابرقدرت‌ها به سرعت در حال توسعه‌ی رزم مبتنی بر شبکه و قابلیت‌های نظامی خود در این حیطه هستند تا بتوانند اقدام به پیاده‌سازی عملیات نتیجه‌محور نمایند. این کشورها انتظار دارند در نبردهای مشترک آتی بتواند با کمک قدرت حاصل از رزم مبتنی بر شبکه به مزیت رقابتی دست یابند (Cebrowski and Garstka, 1998).

رزم مبتنی بر شبکه به کمک شبکه‌ای از حسگرها، تصمیم‌گیرندگان و تفنگداران، میزان آگاهی، و سرعت انتقال فرامین و همزمانی را در درگیری‌های تن به تن افزایش داده و توانایی کشتار دشمن و شانس نجات نیروهای خودی را ارتقا می‌دهد این سیستم‌ها با برقراری ارتباط مؤثر میان نیروهای حاضر در میدان جنگ، آگاهی آنها را به شدت بهبود می‌بخشند و اتخاذ تصمیمات در همه‌ی رده‌های نظامی را تسهیل و تسریع می‌کنند، و در نهایت منجر به افزایش سرعت پیاده‌سازی عملیات و ایجاد مزیت در نبرد می‌شوند (Garstka, 2003).

1 - Effect-based Operation

نتیجه‌گیری

استفاده از چارچوب‌ها (که نظریه‌هایی برای تحلیل هستند) از الزامات نظری آن‌دسته از حوزه های علمی به شمار می رود که شناخت و درک نسبتاً کمی درباره پدیده‌های تحت بررسی آنها وجود داشته و چیستی پدیده‌های مورد نظر به خوبی تبیین نشده است. در واقع چارچوب‌ها به جای توجه بر روابط بیرونی یک پدیده با سایر پدیده‌ها و نحوه تأثیر و تأثر آنها، بر چیستی آن پدیده و تبیین روابط درونی آن تأکید دارند. رزم اطلاعاتی از جمله مفاهیمی است که در حوزه‌ی علوم دفاعی و امنیتی تعابیر گوناگونی درباره چیستی آن ارائه شده و وجه تمایز مشخصی بین تعابیر و کارکردهای گوناگون آن وجود ندارد. بنابراین این مفهوم نیازمند پشتیبانی با چارچوب‌های نظری است که به تبیین چیستی و روابط درونی آن بپردازد.

در واقع، پیچیدگی‌های حوزه رزم و حوزه فناوری اطلاعات موجب پیچیدگی مضاعف رزم اطلاعاتی و مفاهیم مرتبط با آن، که حاصل به‌کارگیری فناوری‌های اطلاعاتی در حوزه‌ی دفاعی می‌باشد، گردیده است. این امر موجب شده تا مفاهیم متعددی در حوزه‌ی رزم اطلاعاتی شکل گیرد که برخی از این مفاهیم با سایر موارد هم‌پوشانی داشته و مرزبندی مشخصی بین آنها وجود ندارد. از این رو، به‌منظور مفهوم‌سازی رزم اطلاعاتی و ساختاردهی به مفاهیم مربوطه، چارچوب رزم اطلاعاتی ارائه گردید. این چارچوب، از سه محور «جهت رزم اطلاعاتی»، «عمق رزم اطلاعاتی» و «عناصر رزم اطلاعاتی» تشکیل شده است. از تقاطع این سه محور، ۱۲ سلول شکل می‌گیرد که هر سلول بخشی از مفاهیم مرتبط با رزم اطلاعاتی را در خود جای می‌دهد. بر اساس این چارچوب، رزم دانش‌محور در سلول رزم اطلاعاتی تهاجمی مبتنی بر آگاهی و دانش (سلول ۲)، رزم اطلاعاتی راهبردی در سلول رزم اطلاعاتی راهبردی تهاجمی مبتنی بر داده و اطلاعات (سلول ۸) و رزم اطلاعاتی مبتنی بر شبکه در سلول رزم اطلاعاتی تهاجمی مبتنی بر فناوری (سلول ۱۲) قابل تقسیم بندی می‌باشد. به‌کارگیری این چارچوب موجب شکل‌گیری تفکر ساختاریافته درباره مفاهیم مرتبط با رزم اطلاعاتی شده و محققان را در راستای شناسایی و تحلیل شکاف‌های موجود در این حوزه پشتیبانی می‌نماید.

منابع

انگلیسی

1- Basden, A. (2008), "***Philosophical Frameworks for Understanding Information Systems, IGI Publishing***", Hershey, New York.

2- Casper, L., Halter, I. (1996), "***Knowledge-Based Warfare: A Security Strategy for the Next Century***", JFQ.

3- Cebrowski, A. K. and Garstka, J. (1998), "***Network-Centric Warfare: Its Origin and Future***", U.S. Naval Institute Proceedings. Annapolis, Maryland: January.

4- Connery, D. (2003), "***Trash or Treasure? Knowledge Warfare and The Shape Of Future War***", National Library Of Australia, Strategic and Defence Studies Centre.

5- Cronin, B., & Crawford, H. (1999), "***Information warfare: Its applications in military and civilian contexts. Information Society***", 15(4), 257264.

6- Edward A. Smith, Jr., (2002), "***Effects-Based Operations: Applying Network-Centric Warfare in Peace, Crisis, and War***", Washington, DC: DoD CCRP.

7- Evans, M. (2012), "***Knowledge Management and Warfare in the Information Age***", Land Warfare Studies Centre.

8- Garstka, J. (2003), "***Network-Centric Warfare Offers Warfighting Advantage***", Signal.

9- Gompert D. (1999), "***Right Makes Might: Freedom And Power In The Information Age***". Rand Research.

10- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005), "***Tenth Annual, 2005 CSI/FBI Computer Crime and Security Survey***", San Francisco: Computer Security Institute (www.gocsi.com).

11-Gregor, S. (2006), "***The nature of theory in information systems***", MIS Quarterly, Volume: 30, Issue: 3, Publisher: Citeseer, Pages: 611-642.

12-Gregor, S. (2009), "***Building Theory in the Sciences of the Artificial***", Academy of Management Review.

13-Halpin, E., Trevorrow, P., Webb, D. and Wright, S. (2006), "***Cyberwar, Netwar and the Revolution in Military Affairs***", Palgrave, Macmillan.

14-Janczewski, Le., Colarik, A. (2008), "***Cyber warfare and cyber terrorism***", Idea Group Inc (IGI).

15-Jones, A., Kovacich, G. L., & Luzwick, P. G. (2002), "***Global information warfare: How businesses, governments, and others achieve objectives and attain competitive advantages***". New York: Auerbach Publications.

16-Lambe, P. (2003), "***The Perils of Knowledge-Based Warfare' in Knowledge Management***", http://www.destinationkm.com/articles/default.asp?ArticleID=1043.

17-Molander, C., Riddile, S. and Wilson P. (1996), "***Strategic Information Warfare: A New Face of War***", Santa Monica, Calif.: RAND, MR-661-AF.

18-Molander, R., P. Wilson, D. Mussington, and R. Mesic (1998), "***Strategic Information Warfare Rising***", Santa Monica, Calif.: RAND, MR-964- OSD.

19-Office of Force Transformation, (2003), "***Network Centric Operations Conceptual Framework***", Version 2.0, See also Network Centric Operations Conceptual Framework, Version 1.0, November.

20-Rattray, G. (2001), "***Strategic Warfare in Cyberspace***", MIT Press.

21-Rhem, K. T. (2005), "***China investing in information warfare technology***", doctrine. American Forces Press Service.

22-Richard Szafranski, (1995), "***A Theory of Information Warfare***", Airpower Journal.

23-Silberglitt, R., Antón, P., Howell, D. (2006), "***The Global Technology Revolution 2020***", In Depth Analyses.

24-Tzu S. (1971), "***The Art of War***". Translated by Ralph D. Sawyer. Boulder, CO: Westview Press, 1994.

25-US Office of the force transformation, (2010), "***The Implementation of Network-Centric Warfare***", Office of the Secretary of Defense.

26-Ventre, D. (2009), "***Information Warfare***", Wiley – ISTE.

27-Ventre, D. (2011), "***Cyberwar and Information Warfare***", Wiley – ISTE.