فضای سایبر، قدرت هوشمند با رویکرد پدافند غیرعامل

حسن حسینی امینی[1]، امیر محسن زادگان[2]

چکیده

رویکرد پدافند غیرعامل مجموعه فنونی را در خود نهفته دارد که می‌تواند در عرصه نبرد نامتقارن مزیت و برتری به کشورهای کمتر پیشرفته در عرصه فناوری‌های ارتباطاتی اعطا نماید، و همچنین پایه‌ای برای ارتقای قدرت هوشمند کشورها در چارچوب اشکال متحول شده نبرد باشد. در این مقاله با توجه به امر فوق به تبیین اشکال متحول شده نبرد در پیوند با فناوری‌های ارتباطاتی و اطلاعاتی پرداخته شده، نقش پدافند غیرعامل در ارتباط با این عوامل بررسی شده است. در بخش دیگری از این نوشتار پس از ذکر ابعاد مختلف نبرد در قالب‌های سخت و نرم به بررسی مفهوم کارآمدی و خصلت مشروعیت سازی آن به‌عنوان سوژه‌ای برای عملیات روانی متخاصمان در عصر جهانی شدن پرداخته شده است. هدف اصلی مقاله شرح و تبیین شیفت پارادایمی در روش‌ها و فنون حفاظتی، امنیتی و دفاعی با توجه به دگرگونی‌های فناورانهٔ عصر کنونی می‌باشد و بر این مبناست که بر در پیش گیری شیوه و ابزار مناسب پدافند اطلاعاتی در عصر تصویر سازی در مقابله با عملیات روانی دشمن تأکید شده است. بر این مبنا در این اثر دگرگونی شیوه‌های نبرد و پدیدار شدن اشکال جدید اجتماعی جنگ و کیفی شدن این شیوه‌ها و ابزارها، پدیداری حیطه‌های نوین نبرد، تعیین کنندگی ساختار و سازمان و فناوری در پدیداری اطلاعات راهبردی ترسیم شده است. در این راستا چگونگی استقرار سازمان‌ها و نهادهای پدافندی و قرارگاه‌های سایبری در چارچوب دکترین دفاعی در فضای سایبری بر مبنای قدرت هوشمند واکاوی گشته؛ درنهایت نیز مدل برخورد در عصر استیلای قدرت هوشمند که مدلی تلفیقی و مشتمل بر ترکیب قدرت فیزیکی و سخت با قدرت مجازی و رسانه‌ای می‌باشد که به نوعی منطق قدرت را به منطق تکثیر تبدیل می‌نماید ترسیم شده است.

کلیدواژه ها: قدرت هوشمند، همگرا و مضاعف، جنگ نرم، جنگ روانی، عملیات روانی، جنگ رسانه‌ای.

---

۱. مدرس دانشگاه و دانشجوی دکترای جغرافیا و برنامه ریزی شهری

۲. مدرس دانشگاه و دانشجوی دکترای جغرافیا و بر نامه ریزی شهری

«مقدمه »

مولفه و پارامتر مهم و تاثیرگذاری که در دگردیسی ماهوی و شکلی مفهوم دفاع غیرعامل و مفاهیمی چون سازمانهای دفاع شهری و دفاع غیرنظامی از اشکال سنتی و کلاسیک آن در اواسط قرن بیستم تا اشکال نوین و فرامدرن آن در قالب جنگهای نوین در قرن کنونی، قرن بیست و یکم نقش داشته است، پویایی‌های تکنولوژیک به ویژه انقلاب مایکروالکترونیک جدید (به تعبیر تافلر موج سوم تکامل زمان) در نظام فراصنعتی بوده[۱] که در این حوزه در قالب جنگهای اطلاعاتی، جنگهای سایبری، جنگ روانی، جنگ رسانه-ای، عملیات روانی و... پدیدار و متجلی شده است. در این راستا به عنوان یک مفروض می‌توان ادعا نمود که روشها، شیوه‌ها و مفاهیم مرتبط با قدرت نظامی دچار تحولی بنیادین شده است و مفاهیم و شیوه‌های متفاوتی از نبرد و قدرت نظامی که در بالا ذکر شد را شاهد هستیم. به واقع در چارچوب نظم فراوستفالیایی می‌توان بیان داشت که شبکه‌های غیررسمی به طور عام و در قالب فضای مجازی و اینترنت (که به نوعی خود یک قاره پنداشته شده) به طور خاص مدیریت این جهان به هم وابسته را به دست گرفته‌اند و سرزمینی بودن روابط بین‌الملل سنتی و بازیگر اصلی آن یعنی دولتها را به چالش کشیده‌اند.

در این فضای مجازی ما با تحول در مفاهیم پیشین و قبض و بسط آنها مواجه‌ایم یعنی قدرت از حالت شخصی شدن[۲] به حالت رسانه‌ای شدن[۳] سوق یافته است که موجب حاکم شدن نگرش تعاملی – توافقی – رقابتی - تفاهمی[۴] بر نظام کنونی بین‌الملل شده و در دنیای وابستگی متقابل پیچیده و در عصر انقلاب اطلاعات و ارتباطات، مرزهای ملی رسوخ پذیر شده است. در این راستا می‌توان گفت حقوق ملتها بر حقوق دولتها ارجحیت یافته و به گفته هانری لوفور، انسان سایبرنیتیک جایگزین انسان رومی شده است و به نوعی مفاهیمی چون فرهنگ شهروندی شبکه‌ای[۵]، دولت الکترونیکی[۶]، جنگ شبکه‌ای[۷]، جنگ اطلاعاتی[۸] و... را پدیدار ساخته و سایبرپولیتیک را به سیاست غالب در اواخر قرن بیستم و آغاز قرن بیست و یکم مبدل ساخته است. این روند ایجاد کشور مجازی و دولت مجازی و شیشه‌ای شدن مرزها و جغرافیا زدایی باعث شده تا عنصر گسترش اطلاعات قدرت را به طور گسترده‌ای پخش نموده و شبکه‌های غیررسمی به انحصارگری بوروکراسی‌های سنتی خاتمه دهند و دیوارهای امنیتی سایبری در قالب دیواره‌های آتش[۹]

---

۱ - انقلاب اطلاعاتی اخیر مبتنی بر پیشرفتهای تکنولوژیکی سریعی است که به طور چشمگیری هزینه تولید، تحلیل و انتقال اطلاعات را کاهش داده است. محاسبات نشان می‌دهد که میزان و حجم قدرت تکنولوژیکی طی ۳۰ سال گذشته هر ۱۸ ماه دو برابر شده است و با آغاز قرن ۲۱ هزینه تولید آن یک هزارم رقم آن چیزی است که در اوایل دهه ۷۰ بوده است. (نای، ۱۳۹۰، ۲۵۸)

2 - Personification
3 - Viediatisation
4 - Coopetition
5 - Netizen Culture
6 - E-government
7 - War of Networks
8 - Information Warfare
9 - Firewall

جایگزین دیوارها و دژهای دفاعی احداث شده در طول تاریخ بشری چون دیوارچین، دیوار برلین، دیوار ماژینو، دیوار آتلانتیک و... شوند. در واقع با وجود تسلیحات هوشمندی چون بمبهای الکترومغناطیسی، نوترونی و گرافیتی دیوارهای سخت بتونی بلااثر و نفوذپذیر شده و همگام با تغییر روشهای تهاجم روشهای حفاظت نیز تغییر یافته و دچار تغییرات ماهیتی شده است. امروزه دامنه تاثیرگذاری عنصر اطلاعات و ارتباطات دامنه‌ای وسیع از جنگ نرم و جنگ روانی تا جنگهای اطلاعاتی و سایبری را دربر می‌گیرد، از شبکه‌های اجتماعی چون توییتر و فیس بوک و تارنماهایی چون ویکی لیکس که تاثیرات و پیامدهای امنیتی بسیاری را در نزد افکار عمومی و دولتها و سرویسهای اطلاعاتی بر جا می‌گذارند تا خرابکاری‌های سایبری در رابطه با برنامه‌های هسته ای و هکرها که با شکستن کدها و رسوخ به رایانه‌های سازمانهای مهم و سیستمهای هدف با به کارگیری بد افزارهایی چون استاکس نت و دوکو و فلیم به سرقت اطلاعات محرمانه و فوق سری و طبقه‌بندی شده می‌پردازند؛ که لازمه مقابله با آنها به کارگیری قدرت هوشمند در فضای مجازی می‌باشد که درک پیچیده‌تری از قدرت در سیاست جهانی را در عصر اطلاعات به دست می‌دهد.

«بیان مساله»

دغدغه بنیادی این اثر شرح و تبیین شیفت پارادایمی در روش‌ها و فنون حفاظتی، امنیتی و دفاعی با توجه به دگرگونی‌های تکنولوژیک عصر کنونی می‌باشد یعنی ترسیم گذار از شیوه‌ها و فنون امنیتی-دفاعی کلاسیک عصر جنگ سرد و دوران وستفالی و عصر سیطره و حاکمیت بلا منازع دولتها و غلبه پارادایم مکانیک نیوتنی به شیوه‌ها و روش‌های امنیتی-دفاعی عصر فراوستفالی و دوران غلبه و رواج پارادایم کوانتومی یعنی مشارکت و حضور فعال بازیگران فراملی و فروملی در امور امنیت بین المللی. دراین راستا پرسشی که می‌توان مطرح نمود بر این مبناست که آیا ایستارها و روندها و نگرش‌های سابق کفایت و پاسخگویی به دغدغه‌های امنیتی را برآورده می‌سازد و حافظ هویت‌های وجودی و هستی شناسانه موجودیت‌های سیاسی و کنشگران عرصه بین المللی هست یا خیر؟ و آیا لزوم انطباق و در پیش گیری فنون نوین در فرآیندهای امنیتی،دفاعی و حفاظتی اجتناب ناپذیر است؟

پاسخ موقتی که در قالب یک فرضیه بدین پرسش می‌توان داد اتخاذ بلادرنگ و هوشمندانه ایستارها و فرایندهای نوین و پی ریزی ساختارها و سازمان‌های تدافعی و حفاظتی با توجه به رویکرد پدافند غیرعامل در چارچوب قدرت هوشمند،همگرا و مضاعف در قالب مدل تلفیقی ترکیب قدرت فیزیکی و سخت با قدرت نرم و مجازی در برابر روندها و شیوه‌های نوین و متحول چالش‌ها و تقابلات امنیتی می‌باشد.در واقع در عرصه نبرد نامتقارن سایبری میزانی از بهره مندی از تکنولوژی‌های اطلاعاتی-ارتباطاتی می‌تواند بازدارندگی بسیاری را در این عرصه و حوزه برای کشورها یی که در عرصه‌های تکنولوژیک پیشرو نیستند محقق سازد و مزیت‌ها و بهره مندی‌های بسیاری را در پی داشته باشد و درچارچوب یک معادله هزینه-

فایده گونه کشورها را بهره مند از "امتیاز نامتقارن درگیری در جنگ مجازی" گرداند.

«روش تحقیق و شیوه گردآوری اطلاعات»

فرایند پژوهش در قالب این مقاله بر مبنای شیوه تحلیلی-توصیفی ابتناء داشته؛ روش گردآوری اطلاعات به شکل رجوع به منابع کتابخانه ای می‌باشد.

در بعد معرفت شناسانه و شیوه متدولوژیک نیز رویکرد و رهیافت یافت باورانه(پوزیتیویستی) که بر علت کاوی و توضیح و تبیین پدیده‌ها و ترسیم رابطه بین متغیرها دلالت دارد مد نظر بوده است.

«یافته‌های تحقیق»

-دگرگونی شیوه‌های نبرد و پدیدار شدن اشکال جدید اجتماعی جنگ که در آنها اثری از وجوه عینی و حقوقی جنگ بین دو دولت را نمی بینیم.

-برجسته شدن متغیر کیفیت شیوه‌ها و ابزار امنیتی-دفاعی نسبت به کمیت.

-تحت الشعاع قرار گرفتن عوامل مکانی و زمانی در برابر فضای مجازی. به واقع نبرد در قالب شبکه ای پیچیده رخ می‌دهد و واحدهای نبرد در این قالب آرایش می‌یابند، یعنی در چارچوب نبردهای مدرن و این مدل نبرد،جنگ اطلاعات را می‌توان حیطه نبرد پنجم قلمداد نمود.

-اهمیت تعیین کنندگی ساختار و سازمان و فناوری در پدید آوردن اطلاعات راهبردی که به صورت یک دارایی راهبردی پدیدار شده است. و سبب شده عملیات نظامی با توانایی مسلط شدن بر عملیات "اطلاعات-تسلط" صورت پذیرد تا پیروی از راهبردهای اصطکاک و مانوری گذشته. در اینجا ابعاد روانی و سازمانی جنگ سایبری به اندازه ابعاد فنی اهمیت دارد.

-در بعد دگرگونی در سطوح تحلیل می‌توان بیان داشت:از منظر گفتمان مسلط واقع گرایی دولت نقش بی بدیلی در مسائل امنیتی و سیاست حاد داشته است. ظهور و بروز کنشگران فرو ملی و فرا ملی و افراد در عرصه جهانی و بدل شدن آنها به بازیگران موءثر در این عرصه و ظهور پدیده هایی همچون تروریسم مجازی در قالب هویت‌های افراد و گروه‌های غیر دولتی عدم کفایت دیدگاه مسلط و فراروایت روابط بین الملل را نشان می‌دهد.

-دستاوردهای کاربردی و انضمامی در راستای رویکرد پدافند غیرعامل اطلاعاتی:بیان روش‌ها و الگوها و تجارب سایر کشورها در مورد پی ریزی سازمان‌ها و نهادهای دارای رویکرد پدافند غیرعامل و چگونگی عملکرد قرارگاه‌های سایبری،بهینه کردن کارکرد این سازمان‌ها با اندیشه خلاق دفاعی و تدوین دکترین دفاعی در فضای سایبری،تعیین نقش‌ها و مسوولیت‌ها در راستای پی ریزی امنیت مجازی برای اجرای امنیت ملی بر مبنای قدرت هوشمند در راستای رسیدن به هدف توان بازدارندگی در حوزه سایبری و ایجاد یگان‌های ویژه و تدوین قوانین لازم برای قدرت بخشی عملکرد سازمان در راستای مهار تروریسم مجازی.

–جنگ نرم مقدمه ای برای جنگ سخت است.اولویت اقدامات پدافند غیرعامل باید بر مقابله با محورهای تهدید نرم متکی باشد.

–اشکال مختلف جنگ نرم با اقدامات روانی و تبلیغات رسانه ای در صدد آن است بدون درگیری نظامی و گشوده شدن آتش رقیب را به انفعال و شکست وادارد و این امر با تغییر باورها،ارزشها،برداشتها،عقاید و احساسات در جامعه هدف و کسب مشروعیت و جذابیت برای دشمن به منظور نفوذ در اذهان مخاطبین بوسیله ابزارهای نرم (که مشتمل بر استفاده حساب شده تبلیغات و شعارها بر ضد حریف است) صورت می‌گیرد.

–تلفیقی شدن مدل برخورد در عصر استیلای قدرت هوشمند همگرا.یعنی شاهد ترکیب قدرت فیزیکی و سخت با قدرت مجازی و رسانه ای هستیم و در واقع انباشت تمامی توانهای پراکنده در محیط قدرت را مشاهده می‌نماییم،که به نوعی منطق قدرت را به منطق تکثیر مبدل نموده است.در این راستا تصویر و زبان همگانی دیجیتالی و اشکالی از رسانه‌ها که دارای ویژگی‌های پیچیدگی و فراگیری اند همواره در طرح‌های استراتژیکی برای هر عملیاتی موضوعیت می‌یابند.

	سنتی و کلاسیک	**نوین و فرامدرن**
هستی شناسی:	مبتنی بر بازیگران ملی و دولت محوری پارادایم مکانیک نیوتنی	مبتنی بر بازیگران ملی،فرو ملی،فراملی و ذرهای پارادایم مکانیک کوانتومی
اشکال نبرد:	اشکال سنتی جنگ	اشکال مدرن اجتماعی جنگ
بعد و فضای درگیری:	زمین،هوا،دریا،فضا	حیطه نبرد پنجم فضای مجازی و اطلاعاتی
شیوه‌های نبرد:	عملیات بر اساس پیروی از راهبردهای اصطکاک و مانوری	توانایی مسلط شدن بر عملیات "اطلاعات–تسلط"
نقش عوامل مکانی و زمانی:	غلبه ژئو پلتیک قدرت	حاکم شدن روند هایی چون جغرافیا زدایی، شیشه ای شدن مرزها،به چالش کشیده شدن زمان و مکان توسط فضای مجازی، غلبه اکوپلتیک قدرت و سایبر پلتیک امنیت ملی
ابزار:	نبرد متعارف با تسلیحات واجد فناوری‌های سطح پایین	نبرد غیر متعارف بر مبنای تسلیحات دارای فناوری نسل چندم
نوع قدرت:	قدرت سخت	قدرت تلفیقی

جدول تبیین کننده تحول و دگرگونی در نبرد در عصر قدرت هوشمند با تکیه بر نقش فناوریهای ارتباطاتی و اطلاعاتی

۱- جنگ اطلاعاتی

هم اکنون مباحثه بسیار پویایی در مورد تغییرات ایجاد شده به وسیله انقلاب ارتباطاتی و اطلاعاتی در بخش نظامی و امنیتی مطرح می‌باشد. بر طبق این مباحثات توسعه فناوری اطلاعاتی و ارتباطاتی شیوه نبرد را به همان نسبتی که ابزارهای نیروهای امنیتی و نظامی را تغییر داده با پی‌ریزی ساختار مجدد، دستور کار حاکم بر امور نظامی بین المللی را نیز متحول ساخته است. در این راستا، انقلاب ارتباطاتی و اطلاعاتی مستقیماً با انقلاب در مسائل نظامی[1] مرتبط است. در عصر ارتباطات، قدرت نظامی به صورت ساده پیشین همان قدرت نیروی آتش نیست بلکه به وضوح و دقت ساز و کار تسلیحاتی مربوط می‌شود. دقت ساز و کارهای تسلیحاتی با اطلاعات پیچیده و پیشرفته، قدرت نظارت و C_4[2] (فرماندهی، کنترل، ارتباطات و رایانه) مرتبط است و در این رقابت بر سر سیستم تسلیحاتی عایدی و بهره طرفی که به واسطه سازمانها و فناوری‌های پیشرفته اطلاعات مهم راهبردی را به دست آورده است بیشتر است. در واقع آنچه در بالا بیان شد رابطه نزدیک میان قدرت نظامی و قابلیتهای جمع‌آوری اطلاعات و تغییرات در راهبردهای فرمول بندی شده را انعکاس می‌دهد در این راستا پیش شرط یک نبرد در عصر اطلاعات وجود واحدهای نبرد در قالب شبکه بسیار پیچیده می‌باشد که نبرد شبکه‌ای در عصر اطلاعات را محقق می‌سازد. از آنچه بیان شد می‌توان نتیجه گرفت که خود اطلاعات امروزه به صورت یک دارایی راهبردی پدیدار شده که اهمیت آنچه به نبرد اطلاعات موسوم است را به یک نوع مشروع از نبرد سوق می‌دهد. هدف نهایی نبرد اطلاعاتی که در قرن بیست و یکم پیش بینی می‌شود شدت یابد دستیابی به مزیت رقابتی در اطلاعات به وسیله اختلال در ساز و کار اطلاعاتی و شبکه‌های رایانه‌ای دشمن می‌باشد. مقیاس نبرد اطلاعاتی امروزه کاملاً تغییر یافته و طیفی از نفوذ به شبکه رایانه‌ای دشمن تا حتی تهاجم به سیستمهای باوری و ارزشی دشمن را شامل می‌گردد. در واقع این کارکرد در عصر اطلاعات معنای امنیت را که ورای تعریف ساده نظامی آن می‌باشد و برابر با تاثیرگذاری در عرصه نامحسوس عقاید و ارزشهاست بازتاب می‌دهد. آنچه توجه ما را به این تغییرات جلب می‌نماید آن است که مفهوم انقلاب اطلاعات و ارتباطات در بطن ساز و کارهای تسلیحاتی، مفهوم راهبرد و نوع نبرد جای دارد و واقعیت آن است که فناوری اطلاعاتی کشورهای کمتر قدرت یافته، گروه‌های مشخص و حتی افراد را قادر نموده تا به سهولت به حمله یا ضدحمله بپردازند. حتی ابرقدرتهایی مانند امریکا نیز در برابر چنین حملاتی آسیب‌پذیرند. (JaBae, 2003:84)

1 - Revolution in Military Affairs (RMA).
2 - C4 (Command, Control, Communication, Computer)

در این راستا می‌توان بیان داشت که به برکت تغییرات فناوری و به طور عام‌تر شیوه تولید، توانایی انجام جنگ متعارف به طور فزاینده به توانایی کشور در جذب فناوریهای نوظهور در عملیات نظامی کشور به ویژه توانایی آن در مسلط شدن بر عملیات «اطلاعات — تسلط» بستگی دارد. توانایی بهره‌برداری از انقلاب فناوری اطلاعات به دارندگان این فناوری برتری‌های بزرگی می‌بخشد (به ویژه نسبت به رقبایی که هنوز اسیر پیروی از راهبردهای اصطکاک و مانوری هستند که در گذشته مورد توجه بود). (تلیس و دیگران، ۵۴:۱۳۸۳)

با توجه به آنچه در بالا ذکر شد می‌توان جنگ اطلاعاتی در چارچوب پدافند غیرعامل یا پدافند عامل اطلاعاتی را بدین صورت تعریف نمود: «جنگ اطلاعاتی یک ویژگی درگیریهای نظامی است که سیستمهای اطلاعاتی به طور مستقیم و یا غیرمستقیم مورد تهاجم واقع شده یا از آنها دفاع می‌شود تا بدین ترتیب داده‌ها، دانش، باورها یا پتانسیل جنگجویی دشمن افت کرده یا کاملاً نابود شود و در عین حال داده‌ها، دانش، باورها و میل به جنگجویی نیروهای خودی حفظ شود.» (اسکندری، ۱۰۸:۱۳۸۹) جنگ اطلاعاتی که تعریف مفهومی‌اش را از نظر گذراندیم در دو حوزه اصلی «اطلاعاتی — روانی» و «اطلاعاتی — فنی» به عملیات می‌پردازد. پرواضح است که درگیری در حوزه اطلاعاتی — روانی که عمدتاً یک درگیری استراتژیک محسوب می‌شود، بر فرایندهای اطلاعاتی انسان متمرکز است در حالی که در حوزه اطلاعاتی — فنی که از تاثیری تاکتیکی برخوردار است، جریان اطلاعات در سیستمهای فنی دخیل در فرایندهای اطلاعاتی انسان را هدف قرار می‌دهد. (کمیته پدافند غیرعامل آموزش و پرورش، ۱۱۶:۱۳۸۸) جنگ اطلاعات در نبردهای مدرن به عنوان یک مدل جنگی مستقل و کاملاً اثرگذار درآمده است و حتی می‌توان آن را پس از زمین، هوا، دریا و فضا حیطه نبرد پنجم دانست آن گاه بدیهی است که این مدل جنگی جدید از ویژگیهای شناخته شده متفاوتی برخوردار باشد. بررسیها نشان می‌دهد که هفت ویژگی اصلی را می‌توان برای جنگ اطلاعات برشمرد: ۱- گستردگی ۲- همه جانبه گرایی ۳- کیفی بودن ۴- اخلالگری ۵- عدم تقارن ۶- بعد زمانی نامحدود ۷- سرعت محوری (برای آگاهی بیشتر از هر یک از مفاهیم ذکر شده ر.ک.: منبع پیشین، ۱۱۸-۱۲۰)

ویژگیها و ماهیت هر مدل جنگی معمولاً سبب بروز رخ دادهایی می‌گردد که از این رخدادها به نام «پدیده» یاد می‌شود. مرگ آگاهی، ناتوان سازی استراتژیک (واپاشی سیستمی) و برتری اطلاعاتی از جمله پدیده‌های اصلی قابل شناسایی در جنگ اطلاعاتی‌اند. (برای آگاهی بیشتر ر.ک: منبع پیشین، ۱۲۱ و ۱۲۲)

ارتباط جنگ اطلاعات و پدافند غیرعامل را می‌توان در دو حوزه اصلی «پدافند غیرعامل اطلاعاتی» و «اثر عملیات اطلاعاتی بر پدافند غیرعامل» بررسی نمود.

۱-۱- پدافند غیرعامل اطلاعاتی

پدافند غیرعامل اطلاعاتی را می‌توان مجموعه ساز و کارهایی قلمداد کرد که می‌توانند مانع اجرای عملیات اطلاعاتی دشمن شده، از شدت آسیب رسانی آن بکاهند و یا حتی پس از اعمال اثر اطلاعاتی دشمن، توان رزم خودی را حفاظت نمایند. در این مدل تدابیر و اقدامات پدافند غیرعامل، به نحو تخصصی بر توان خود در مقابله با تهدیدات اطلاعاتی می‌افزایند. به عنوان مثال حفاظت اطلاعات تنها بخشی از مجموعه وسیع راه کارهای ضروری برای مقابله با تهدیدات اطلاعاتی به شما می‌رود. یادآوری این نکته ضروری است که یکی از مهمترین تمهیدات پدافند غیرعامل اطلاعاتی، کاهش آسیب‌پذیری زیر ساختهای حیاتی اطلاعات در سطح ملی است. (پیشین: ۱۱۴)

۲-۱- اثر عملیات اطلاعاتی بر پدافند غیرعامل

اثرات عملیات اطلاعاتی دشمن بدون تردید می‌تواند بر جنبه‌های مختلف عملیات پدافند موثر واقع گردد. برخی از این موارد عبارت‌اند از:

۱- تغییر اولویتهای پدافند غیرعامل

۲- در اختیار گذاردن منابع علمی نادرست و جهت‌دار در حوزه پدافند غیرعامل

۳- ممانعت از درک لزوم رعایت الزامات جنگ مدرن (جنگهای اطلاعاتی محور) در اتخاذ راهکارهای پدافند غیرعامل.

۴- جلوگیری از گسترش روشهای نوین پدافند غیرعامل.

۵- شناخت و مقابله با عملیاتهای اطلاعاتی دشمن بر علیه طراحان، مدیران و فعالان پدافند غیرعامل.

۶- شناخت اولویتهای کاری صحیح در محیط تغییر یافته درگیری جنگ مدرن.

در واقع اثرپذیری پدافند غیرعامل از عملیات اطلاعاتی ناشی از اجرای چند عملیات اصلی و عمده اطلاعتی من جمله عملیات علمی دانشی، عملیات روانی و عملیات فریب است. رعایت ملاحظات نبرد اطلاعاتی که از محیط اطلاعات – محور جنگهای امروزی منشعب می‌شود، ضرورتی است که کارآیی تمامی راهکارهای پدافند غیرعامل بدون تردید مستقیماً به آن وابسته است.

الزامات محیط اطلاعات جنگهای مدرن، توسعه نسل جدیدی از راهکارها و مفاهیم پدافند غیرعامل را ضرورت می‌بخشد که حتی شاید مشابه مبانی پذیرفته شده امروزی که عمدتاً مربوط به نسل جنگهای غیراطلاعاتی هستند، نیز نباشد. (پیشین: ۱۱۵)

۲- جنگ سایبری

برای تفهیم جنگ سایبری ابتدا باید فضای سایبری و عناصر آن را درک نماییم. بنابراین ابتدا باید ببینیم اصولاً سایبر به چه معنایی است. سایبر پیشوندی برای اسامی متعدد و متنوعی است که همگی براساس انتشار

روزافزون رایانه پدید آمده‌اند. ضمناً اغلب عناصر درگیر با اینترنت با این پیشوند در ارتباط می‌باشند. اولین اصطلاح در این وادی، فضای سایبری است که استعاره‌ای برای حضور غیرفیزیکی تشکیل شده توسط سیستمهای رایانه‌ای است. بر اساس این تعریف، جنگ سایبری در لغت به معنای تهاجم بر عناصر سایبری است و اصطلاحاً به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستمهای اطلاعاتی با هدف به مخاطره انداختن عناصر اطلاعاتی (اطلاعات، فرآیندهای مبتنی بر اطلاعات، سیستمهای اطلاعاتی، شبکه‌های رایانه‌ای) دشمن در یک فضای سایبری است. چنین عملیاتی به طور مشخص با اهداف نظامی، سیاسی، فرهنگی و ... انجام می‌پذیرد. بنابراین باید دارای ارزش افزوده و به اصطلاح، بهره‌برداری از عناصر دشمن را شامل شود کما این که هر نوع جنگ دیگر نیز نهایتاً به سوء استفاده از منابع دشمن همانند سرقت اطلاعات استراتژیک، اقتصادی، نظامی و... و از کار انداختن سرویسها و خدمات عمومی یا خصوصی ختم خواهد شد. (اسکندری، ۱۱۱:۱۳۸۹) در واقع نبرد سایبری از زیر شاخه‌های اشکال جدید اجتماعی جنگ همانند حملات اطلاعاتی به زیرساختهایی مانند برق، ترافیک هوایی، ارتباطات مالی شبکه‌های خط لوله نفت و گاز می‌باشد که نتیجه آن خنثی شدن بسیاری از شبکه‌های حساس بدون هر نوع انهدام فیزیکی می‌باشد. در این شیوه از نبردهای سایبری مهاجمان رایانه‌ای به وسیله فلج کردن و گسترش اغتشاش و سوء ظن به آلوده سازی نظام فرماندهی و کنترل انسانی اقدامات خود را دنبال نموده، مثلاً فرمانهایی از یک فرماندهی کل قلابی صادر می‌کردند و اخبار و گزارشهای تقلبی از بحران و ویرانی‌ها، از سوی مقامات شهری صادر می‌نمودند و این موجب درهم ریختگی و سردرگمی در سطوح مختلف فرماندهی و کنترل می‌گشت. (جیمز آدامز، ۷۱۵:۱۳۸۰)

بر این پایه می‌توان گفت اصلی‌ترین و اثرگذارترین تغییر فناوری که توانسته است اکثر رویه‌های معمول جنگی را تحت تاثیر قرار دهد و دگرگون سازد معرفی فناوری‌ها مفاهیم عملیاتی نوین در حوزه فرماندهی و کنترل است. در واقع می‌توان C_4HSR[1] را سیستم عامل نرم افزاری – مغز افزاری مدیریت در صحنه دانست که زمینه برتری اطلاعاتی و شناختی را از طریق تعامل پذیری و شبکه سازی تمام عناصر اطلاعاتی و دانشی دخیل در فرماندهی و کنترل فراهم آورده و امکان برقراری ارتباطی سالم و امن در چگال‌ترین زمان ممکن بین نیروهای صحنه نبرد و فرماندهی را ایجاد می‌کند تا تصویر همه جانبه‌ای از فضای نبرد پدیدار شده و مدیریت جبهه امکان پذیر گردد. در قالب جنگ اطلاعاتی و نبرد سایبری و حملات مجازی می‌توان با استفاده از حجم انبوه اطلاعات آلوده پراکنده باعث سردرگمی و اغتشاش نیروهای دشمن شد همچنین با استفاده از این حربه‌ها می‌توان فشار روانی شدیدی بر تصمیم گیری و عملیات دشمن وارد نمود، کاهش شدید اعتمادپذیری به نیروها و امکانات خودی را به وجود آورد و در نهایت باعث مرگ فکری فرماندهان ارشد و میانی شد. (نباتی، ۱۳۸۸ : ۳۹-۴۰)

1 - Command, Control, Communication, Computer & Intelligence, Search & Rescue.

مهمترین ابزارهای جنگ سایبری عبارتند از: ویروسهای کامپیوتری، کرمها، تروجانها، راه‌های پنهان نرم افزاری و سخت افزاری اجرای روندهای ناخواسته در سیستم دشمن. استفاده از چنین ابزارهایی که ماهیتی متفاوت از ابزارهای پیشین جنگی دارند، به بازیگران جنگ سایبری امکان این را داده‌اند که بدون پذیرفتن هزینه‌های حقوقی و مالی و سیاسی و اجتماعی یک جنگ تمام عیار، به بخش مهمی از اهداف خود بدون جنگ دست پیدا کنند.

در باب اهمیت این نوع جنگ در مقایسه با اشکال دیگر نبرد محققان این عرصه اذعان دارند که این نوع جنگ اگر با اهمیت‌تر از اشکال دیگر نبرد نباشد، اهمیت کمتری ندارد و در شرایطی که منابع دانش و اطلاعات، ثروت و قدرت در فضای مجازی به نحو بی‌سابقه‌ای افزایش یافته است، نحوه کنترل این منابع قدرت و نحوه باز تولید و باز توزیع آن و تاثیر این روند بر شکل گیری نقشه و زمین بازی جنگ، دارای اهمیت روزافزونی در حوزه سیاست شده است.

در انتها باید خاطر نشان نمود که اگر چه طراحی و اجرای تمام عیار یک جنگ سایبر مستلزم دسترسی به فناوری پیشرفته است اما جنگ سایبر به خودی خود به فناوری پیشرفته وابستگی قطعی ندارد. در واقع برای جنگ سایبر فقط حضور فناوری پیشرفته الزامی نیست بلکه ابعاد روانی و سازمانی آن به اندازه ابعاد فنی اهمیت دارد. در تحت شرایط خاص شاید واقعاً بتوان با استفاده از فناوری سطح پایین یک جنگ سایبر را آغاز کرد. (اسکندری، ۱۱۳:۱۳۸۹)

۱-۲- به کارگیری قدرت هوشمند در فضای مجازی

امنیت مجازی معمولاً به شکلی ساده انگارانه، امنیت شبکه اطلاعات و سیستمها تعریف شده است ولی حملات عدیده‌ای که بر شبکه‌های حیاتی مالی، دولتی و نظامی وارد شده، تروریسم مجازی را تبدیل به یکی از اولویتهای امنیت ملی کشورها ساخته است. چهار بعد از عملیات انجام شده در فضای مجازی برای امنیت ملی مهم هستند: ۱- ساختن و حفظ فضای مجازی، ۲- اطمینان از آزادی عمل در فضای مجازی، ۳- گرفتن این آزادی از دشمنان و ۴- ایجاد تاثیرات فضای مجازی در تمامی زمینه‌ها.

البته از این ویژگیها تنها اولین آنها مختص فضای مجازی است و سه مورد دیگر در بقیه زمینه‌ها هم لازم الاجرا هستند. در نتیجه به علت ثابت بودن این سه مورد اطلاعات ما از اهداف مورد نظر در فضای مجازی ارتقا می‌یابد. درست مثل دیگر تهدیدات نامتعارف باید روشهایی از به کارگیری قدرت هوشمند و ابزار مورد نیاز آن در فضای مجای موجود باشد.

دولت امریکا که متوجه اهمیت و محدودیتهای موجود در منابع و ساختارهای امنیت مجازی شده بود، چندی قبل «سزارهای مجازی» را برای مقابله با تهدیدات روزافزون مجازی طراحی کرد. وزارت دفاع هم یگانهای ویژه‌ای برای انجام عملیات مجازی ایجاد کرده است. رئیس جمهور امریکا نیز دستور داد یک

گزارش جامع از فضای مجازی در امریکا به وی ارائه شود، بر اساس این گزارش، «فضای مجازی تمامی زمینه‌های زندگی را تحت تاثیر قرار داده و برای اقتصاد، زیرساختهای عمرانی امریکا، امنیت عمومی و امنیت ملی بسیار مهم است» و نتیجه می‌گیرد که تقویت رهبری فدرال در این حوزه، نیازمند تعیین نقشها و مسوولیتهای آژانسهای فدرال است. همچنین نیاز است قوانین مورد نیاز برای قدرت بخشی به این آژانسها برای اجرای وظیفه‌شان تدوین شود.

برنامه امنیت مجازی دولت به طور قطع شامل یک بازه زمانی خاص برای تدوین و اجرای استراتژی امنیت ملی بر مبنای قدرت هوشمند است. (عمیدیان، ۷۹:۱۳۹۰)

۲-۲- دکترین فضای سایبر و دفاع مجازی

با پدیدار شدن ویروسهای جدید با فناوریهای پیچیده‌تر در فضای سایبری که آغاز دور جدید جنگهای سایبری را نوید می‌دهند لزوم تدوین دکترین دفاعی در فضای سایبری در میان کشورها احساس شده است. این تهدید مختص به کشورهایی خاص نبوده چنان که ژنرال کیت الکساندر فرمانده قرارگاه سایبری امریکا حملات رو به رشد در فضای سایبر را به فضای پنجم درگیری جهانی تشبیه نموده است. در این صورت دستگاه‌های اداری و مدیریتی درصدد تعریف دوباره از محیط امنیتی برآمده‌اند. تهدید حملات الکترونیکی – سیبرنتیکی نیازمند رهبری و اندیشه خلاقی است که راه حلهای جدیدی تولید کند. در این راستا رییس جمهور ایالات متحده امریکا سند راهبردی دفاع سایبری سالهای ۲۰۱۵ تا ۲۰۲۸ را تدوین کرد و به تصویب رساند؛ سندی که در قاره امریکا از آن به عنوان دکترین فضای سایبر یاد می‌شود. بنابر اظهارات فرمانده قرارگاه سایبری امریکا این دکترین کمک خواهد کرد تا شرایطی در نظر گرفته شود که ارتش قادر به گرفتن حالت تهاجمی در برابر تهدیدات سایبری باشد و اقدامات ویژه‌ای را بتواند مدنظر قرار دهد. به گفته این ژنرال ارتش امریکا این دکترین از استراتژی وزارت دفاع برای انجام عملیات در فضای سایبری و استراتژی بین المللی فضای سایبری باراک اوباما پشتیبانی خواهد کرد و فرماندهی سایبری برنامه آموزشی خود را برای کادر نظامی خود به اجرا خواهد گذاشت و این مطلب را که «چگونه در فضای سایبری می‌توانیم عملیات انجام دهیم» مورد توجه قرار خواهد داد. (شفیعی، ۸:۱۳۹۰)

تغییرات فوق را در این راستا می‌توان تحلیل نمود که اگر دستگاه اداری و مدیریتی امریکا، در موضع منسوخ پارادایم جنگ سرد متوقف بماند، موقعیت ایالات متحده به عنوان یک ابرقدرت نظامی به وسیله بازیگران جدید جهان سایبرنتیکی به مخاطره خواهد افتاد. از نظر تدوین کنندگان سندهای ذکر شده امریکا باید بتواند امتیاز نامتقارن درگیری در جنگ مجازی را خنثی کند. (جیمز آدامز، ۷۲۸:۱۳۸۰)

در ایران نیز رییس سازمان پدافند غیرعامل کشور از ابلاغ فرمان تشکیل قرارگاه دفاع سایبری در کشور خبر داده است. تشکیل این قرارگاه در راستای سیاستهای کلی در بخش امنیت فضای تولید و تبادل اطلاعات

است که توسط مقام رهبری ابلاغ شده است. به گفته رییس سازمان پدافند غیرعامل کشور ماموریت قرارگاه دفاع سایبری رصد تهدیدات سایبری علیه زیرساختهای امنیت ملی کشور است، طی سالهای اخیر انتشار ویروسهایی که گفته شده برای تخریب و جاسوسی اطلاعات در سیستمهای اطلاعاتی کشور توسط برخی کشورها صورت گرفته، منجر به تشکیل چنین قرارگاهی شد. از زمان انتشار ویروس استاکس نت و هدف گرفتن اطلاعات نیروگاه هسته‌ای و دیگر صنایع، مسوولان در پی اتخاذ تدابیری ویژه در حوزه دفاع سایبری برآمده‌اند. تحلیل گران شرکتهای رایانه‌ای مک آفی و سیمانتیک ارایه کننده خدمات امنیت رایانه‌ای توافق دارند که ویروس پیشرفته و جدید دوکو به طور آشکار با ماموریت جمع آوری اطلاعات برای حمله به سیستمهای کنترل صنعتی طراحی شده است. همچنین کارشناسان نرم افزاری آزمایشگاه کاسپرسکی در روسیه، یک کرم اینترنتی جدید در ایران و سودان را شناسایی کرده‌اند. به گزارش دویچه وله هدف این کرم اینترنتی جمع آوری اطلاعات از صنایع و نهادهای سیاسی بوده و تاکنون سه مورد در ایران شناسایی شده است. در حقیقت این ویروسها در راستای نبردهای اطلاعاتی موسوم به صنفی یا شرکتی[1] (که به سرقت اطلاعات تجاری و استفاده از دستاوردهای رقبا به سود خود پرداخته) و در سطح آخر نبرد اطلاعاتی جهانی[2] (که به حمله به مراکز مهم جهانی یا کلیت یک کشور با اهدافی فراتر از کسب پول و ضرر به اشخاص و رقبای تجاری سیاسی اشاره دارند) نوشته و پردازش شده‌اند.

در این راستا از سوی فرمانده قرارگاه دفاع سایبری کشور اجرایی شدن سیاستهای نظام در بخش افتا، اعلام هشدارهای ملی در برابر تهدیدات امنیتی کشور و ایمن سازی زیرساختهای کشور نسبت به تهدیدات سایبری و ایجاد توان بازدارندگی در حوزه سایبری بعنوان وظایف این قرارگاه اعلام شده است. تدوین سند دفاع غیرعامل و تولید نرم افزارهای بومی با مشارکت نهادها و ارگانهای دیگر و مانورهای سایبری از دیگر اقدامات در این راستا می‌باشد. (شفیعی، ۸:۱۳۹۰) در حقیقت برای توسعه و حفظ سیستم امنیتی انعطاف پذیر مبتنی بر قدرت هوشمند تمامی بخشهای دولتی باید روشها و اولویتهای خود را با این امر تطابق دهند و این وظیفه هماهنگ کنندگی در فضای سایبری کشور بر عهده این قرارگاه می‌باشد.

۱-۲-۲- سیاستهای کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)

۱- ایجاد نظام جامع و فراگیر در سطح ملی و ساز و کار مناسب برای ایمن سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات و ارتقای مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطاتی در کشور به منظور:

- استمرار خدمات عمومی

1- Corporate Information Warfares

2- Global Information Warfare

- پایداری زیرساختهای ملی
- صیانت از اسرار کشور
- حفظ فرهنگ و هویت اسلامی – ایرانی و ارزشهای اخلاقی
- حراست از حریم خصوصی و آزادی‌های مشروع و سرمایه‌های مادی و معنوی

۲- توسعه فناوری اطلاعات و ارتباطات با رعایت ملاحظات امنیتی

۳- ارتقای سطح دانش و ظرفیتهای علمی، پژوهشی، آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت فضای اطلاعاتی و ارتباطی (افتا)

۴- تکیه بر فناوری بومی و توانمندی‌های تخصصی داخلی در توسعه زیرساختهای علمی و فنی امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی

۵- پایش، پیشگیری، دفاع و ارتقای توان بازدارندگی در مقابل هرگونه تهدید در حوزه فناوری اطلاعات و ارتباطات

۶- تعامل موثر و سازنده منطقه‌ای و جهانی و همکاری و سرمایه گذاری مشترک در حوزه‌های دانش، فناوری و امور مربوط به امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی با حفظ منافع و امنیت ملی

۷- تعیین نهاد متولی و هماهنگ کننده زیر نظر دولت به منظور هدایت، نظارت و تدوین استانداردهای لازم برای حفظ و توسعه امنیت فضای تولید و تبادل اطلاعات و ارتباطات و تهیه پیش نویس قوانین مورد نیاز

۸- فرهنگ سازی، آموزش و افزایش آگاهی و مهارتهای عمومی در حوزه افتا

۹- رعایت موازین شرعی و مقررات قانونی مربوط به حفظ حقوق فردی و اجتماعی در اجرای این سیاستها. (پیشین)

۳- جنگ الکترونیک

در جنگ الکترونیک، از انرژی الکترومغناطیس، جهت کنترل طیف الکترومغناطیسی و تهاجم به دشمن، استفاده می‌گردد (کاربرد نرم کشتاری). کنترل طیف الکترومغناطیسی از طریق حفاظت از سامانه‌های خودی و مقابله با سامانه‌های دشمن حاصل می‌شود. جنگ الکترونیک صرفاً محدود به فرکانسهای رادیویی نمی‌شود و شامل طیف اپتیکی و مادون قرمز نیز می‌گردد.

جنگ الکترونیک یکی از مهمترین عوامل کاهش اصل غافلگیری در حملات دشمن است چرا که نیروها و تجهیزات جنگ الکترونیک قادرند در گستره بسیار وسیع به طور آنی عملیات صورت دهند. تجهیزات الکترونیک قادرند توانایی حمله «عمقی دشمن» در طول عملیاتهای هوا به زمین را به شدت کاهش دهند. این

توانایی از طریق اخلال در سامانه کنترل پرتابه‌ها، سامانه‌های هدایتی مهاجم و قطع هماهنگی میان مهاجم و نیروهای پشتیبانی حاصل می‌آید. در مجموع، جنگ الکترونیک به سه بخش اصلی تهاجم الکترونیک، دفاع الکترونیک و پشتیبانی الکترونیک تقسیم می‌شود. (کمیته پدافند غیرعامل آموزش و پرورش، ۱۲۷:۱۳۸۸)

جنگ الکترونیک ماهیتاً تمرینی است برای بهره‌برداری از فرصت و به کارگیری شتاب تاکتیکی به منظور بهره‌برداری ضعیف دشمن از به کارگیری تسلیحات و سنجنده‌هایش، ضمن آن که با زیرکی طرح تاکتیکی تجهیزات دشمن را ستانده و استفاده از تجهیزات الکترونیکی را از او سلب می‌نماید. از آنجایی که جنگ الکترونیک واکنشی به اقدام مستقیم دشمن است و بر آنچه که دشمن در طراحی و بهره‌برداری از تجهیزات و دانش اطلاعاتی که در اختیار تجهیزات دشمن است و همچنین روش استفاده از این تجهیزات تاثیر می‌گذارد طبیعتاً با بهره‌برداری از سایر سنجنده‌ها و تسلیحات کاملاً متفاوت می‌باشد. (اسکندری، ۱۲۰:۱۳۸۹)

آنچه در بالا مطرح شد شمای کلی از مبحث جنگ الکترونیک را واکاوی می‌نمود. این حوزه و مبحث مطالعاتی و گونه جنگ ابعاد و عمق بسیاری را دربرمی‌گیرد که شاخه‌های مختلفی از علوم و فنون از علوم دفاعی تا علوم مهندسی به تشریح و بسط و اشاعه آن می‌پردازند لذا واکاوی ابعاد تخصصی این رشته از نبرد مجال دیگری به طور خاص می‌طلبد و جهت ارائه چشم اندازی برای تکمیل مباحث این متن به تعریف کلی آن اکتفا نمودیم.

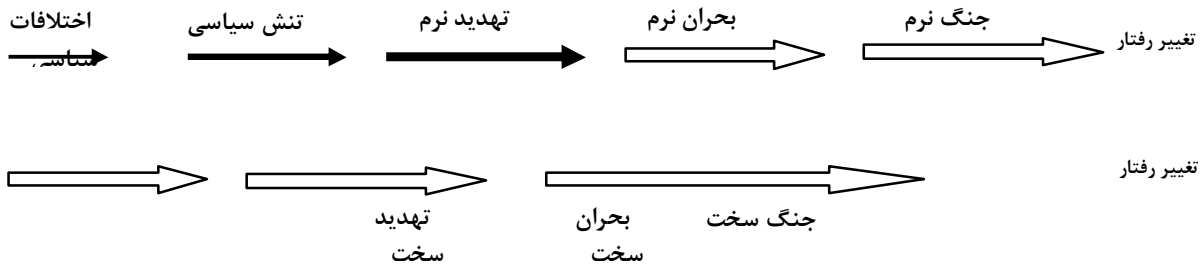
۴- جنگ نرم

در برابر تهدیدات جدید باید دفاع جدید مناسب با همان تهدید را داشت با شناخت تهدیدها و ظرفیتهای خود می‌توانیم راهبردهای خاصی برای مقابله با تهدید داشته باشیم که این همان توسعه مفاهیم و ادبیات پدافند غیرعامل است. به طور کلی سه رویکرد اصلی در توسعه ساز و کارهای پدافند غیرعامل شامل رویکردهای توسعه «تهدید محور»، «قابلیت محور» و «فرصت محور» قابل شناسایی است. در رویکرد تهدید محور، ساز و کارهای پدافند غیرعامل بر اساس محورهای تهدید و به منظور کاهش شدت تهدیدات توسعه می‌یابند یعنی نگاه سلبی حاکم می‌باشد که بازدارندگی و پوشش‌دهی به خلأها و روزنه‌های نفوذ دشمن را مدنظر دارد. در رویکرد قابلیت محور، ساز و کارهای پدافندی بدون توجه ویژه به ماهیت تهدیدات و در راستای ایجاد مجموعه‌ای از قابلیتها توسعه می‌یابند در واقع در اینجا نگاه ایجابی حاکم بوده تقویت و توسعه و پشتیبانی مزیتها و پتانسیلهای درون سیستمی مطمح نظر می‌باشد اما در رویکرد فرصت محور، ساز و کارهای پدافند غیرعامل با ارزیابی دقیق نقاط ضعف دشمن، تلاش می‌کنند این نقاط ضعف را مورد توجه قرار داده و با تضعیف هر چه بیشتر آنها از قابلیتهای دشمن بکاهند. در واقع در این چارچوب نوعی معادله هزینه فایده وجود دارد که بازی با جمع جبری صفر را بازتاب می‌دهد یعنی بهره و تامین منافع ما در گرو

ضرر و از کف رفتن منافع رقیب و طرف مقابل متخاصم است. انتخاب هر یک از این سه رویکرد در ظرف زمانی و مکانی خاص خود به شدت به وضعیت توازن قوای نیروها وابسته است. از طرفی عامل دومی نیز در انتخاب هر یک از رویکردها نقش بازی می‌کند و آن ماهیت پدافند است که اساساً متغیری وابسته به آفند می‌باشد.

به نظر می‌رسد در یک تفکر سامانه‌ای و رویکرد جامع تلفیق و ترکیبی از این رویکردها ارجحیت و برتری داشته باشد و راهگشا باشد و مناسب و قابل انطباق و سازگار با راهبرد قدرت هوشمند یا قدرت همگرا و مضاعف باشد.

از سویی دیگر در مواجهه با انواع و اشکال مختلف تهدید گاهی یک مولفه به ظاهر با درجه اثرگذاری پایین، می‌تواند خارج از معادلات معمول، در تعیین نتیجه جنگ سرنوشت ساز باشد یعنی منطبق با یافته‌های نوین علم مدیریت توان استقامت و پایایی ضعیف‌ترین حلقه از زنجیره اجزاء علی و معلولی فرایندها کلید موفقیت سیستم و گردش مستمر امور و پویایی و بالندگی مجموعه و دریافت بازخوردهای مثبت می‌باشد. در عصر کنونی نیز که با سیالیت و پیچیدگی و ابهام خاص خود حضور متغیرها و مولفه‌های نوینی را نظاره‌گر است شاهد تحول و دگرگونی و دگردیسی در اشکال و ابزار نبرد و بروز و ظهور نسل چندم تسلیحات می‌باشیم. از جمله تکنیکها و ابزارها و شیوه‌هایی که می‌تواند در خدمت توسعه قدرت کشورهای کمتر توسعه یافته نیز قرار گیرد جنبه‌ها و اشکال نرم نبرد در قالب کلی جنگ نرم می‌باشد که در عصر تصویرسازی پنجره‌ها و روزنه‌های متعددی را برای ارتقای سطح قدرت مانور و اعتلای درجه ایفای نقش و بازیگری کشورها در عرصه شطرنج قدرت جهانی در دسترس قرار می‌دهد. در سطور ذیل به کنکاش و واکاوی در باب مفهوم جنگ نرم و تکنیکهای گوناگون آن که می‌تواند خلأ شکاف فناوریهای پیشرفته نظامی و فقدان تسلیحات پیشرفته را در صورت عدم در پیش‌گیری تدابیر پدافندی مناسب مضاعف سازد و در صورت اتخاذ تدابیر مناسب جهت مقابله با جنگ نرم دشمن تمامی تهدیدات اعم از سخت و نرم را خنثی سازد؛ می‌پردازیم. دو گونه اصلی تهدیدات سخت و تهدیدات نرم همواره کشورها را تهدید می‌نماید و کشورها در صورت هرگونه درگیری نظامی احتمالی، در صحنه اصلی جنگ نرم و جنگ سخت به نبرد خواهد پرداخت. روابط این دو گونه از صحنه‌های نبرد مطابق شکل زیر می‌باشد.



شکل ۱- نگاه فازی به جنگ (منبع: کمیته پدافند غیرعامل وزارت آموزش و پرورش، ۱۵۸:۱۳۸۸)

در محیط جنگ نرم، دشمن تلاش می‌کند به کمک ابزارهای نرم همچون تغییر باورها، ارزشها، دیدگاه-ها، تفکرات، حذف روابط میان اعضای جامعه، حذف وحدت و یکپارچگی، استیلای فرهنگی، ایجاد وابستگی علمی و دانشی و بسیاری راهکارهای دیگر بدون اقدام نظامی، دشمن را نسبت به تغییر رفتار و عمل مطابق خواسته‌هایش متمایل سازد. به منظور کسب این هدف دشمن نیازمند کسب مشروعیت و جذابیت به منظور نفوذ در اذهان مخاطبینش است. در وضعیت منطقی، دشمن تا هنگامی که از ناکارآمدی جنگ نرم اطمینان حاصل ننماید احتمالاً به مرحله جنگ سخت یا حمله نظامی ورود نخواهد کرد، اگر چه تهدیدات سخت و حتی ایجاد بحران سخت در دستور کارش باشد. در چنین شرایطی اولویت اقدامات پدافند غیرعامل بر مقابله با محورهای تهدید نرم خواهد بود. (کمیته پدافند غیرعامل آموزش و پرورش، ۱۵۸:۱۳۸۸)

در بسط مفهوم جنگ نرم می‌توان گفت که جنگ نرم در برابر جنگ سخت در حقیقت شامل هرگونه اقدام روانی و تبلیغات رسانه‌ای می‌شود که جامعه هدف یا گروه هدف را نشانه می‌گیرد و بدون درگیری نظامی و گشوده شدن آتش رقیب را به انفعال و یا شکست وامی‌دارد. جنگ روانی، جنگ رایانه‌ای، جنگ اینترنتی، براندازی نرم، راه اندازی شبکه‌های رادیویی و تلویزیونی و شبکه سازی از اشکال جنگ نرم هستند. (اسکندری، ۹۶:۱۳۸۹؛ به نقل از سایت مجلس. ۱۳۸۷)

۱-۴- جنگ روانی

نام بردن از جنگ در جایی که اثری از وجوه عینی و حقوقی جنگ بین دو دولت را نمی‌بینیم می‌تواند با تسامح همراه باشد و می‌توان موضوع را به سطح درگیریها و رقابتهای اطلاعاتی، دیجیتالی، رسانه‌ای، سایبری تقلیل و تنزل داد اما دستگاه‌های عمل کننده در این حوزه تمایل دارند فعالیتهایشان در سطوح بالاتر تصمیم-گیری مورد توجه قرار گرفته و آن را به عنوان بزرگترین مسأله یک کشور حتی مساله‌ای جهانی تلقی می-کنند در واقع می‌توان این گونه جنگها را نوعی رویارویی دانست. صاحب نظران معتقدند طبیعت جنگ در فضای سایبری، دیجیتالی، رسانه‌ای، ارتباطاتی پیوسته در حال تغییر است و جنس این گونه جنگها دچار تغییر می‌شود و همراه با آن، اهداف عملیاتی و ابزارها و عناصر و عمل کنندگانشان نیز دچار تحول می‌شوند هر چند مقاصد نهایی همان اهداف استراتژیک باقی مانده‌اند. (بوترابی، ۳:۱۳۹۰) با این پیش درآمد می‌توان گفت جنگ روانی همان جنگ کلمه و عقیده است، که به صورت مخفی، آشکار، شفاهی و یا کتبی انجام می‌شود. اساساً جنگ روانی سلاحی است که به انسان و عقل او توجه دارد. جنگ روانی عبارتست از یک جریان ارتباطی که در آن دو طرف انسانی شرکت داشته و یک طرف یا هر دو طرف سعی در تاثیر گذاردن بر افکار، عواطف و تمایلات حریف خود (دشمن) و وادار کردن طرف مقابل به انجام رفتاری مطابق خواست

خود که هدف نهایی آنها است، دارد. پل لاینبرگر در خصوص جنگ روانی می‌نویسد: جنگ روانی استفاده از تبلیغات ضددشمن، همراه با اقدامات عملی است که ماهیت نظامی، اقتصادی یا سیاسی دارد.

جنگ روانی مجموعه اقدامات تبلیغی –روانی است که کشور یا گروهی برای اثرگذاری و نفوذ بر عقاید و رفتار دولتها و مردم در جهت مطلوب به پشتیبانی زمینه‌ها و ابزارهای سیاسی، اقتصادی، فرهنگی و نظامی انجام می‌دهند. تفاوت تعریف مذکور با دیگر تعاریف جنگ روانی در نظر گرفتن زمینه‌ها و ابزارهای اقتصادی، نظامی، سیاسی –دیپلماتیک و ارتباطی است. در صورتی که تعاریف متداول بیشتر به ابزارهای تبلیغی –روانی تاکید دارد. به مفهوم دیگر در موضوعهای سیاست خارجی و روابط بین الملل چهار ابزار ۱) نظامی ۲) دیپلماتیک ۳) اقتصادی و ۴) تبلیغی و ارتباطی وجود دارند که در یک تفکر سامانه‌ای، ترکیبی از این چهار عنصر باعث موفقیت می‌شود و کمتر امکان دارد تنها یک عنصر مانند تبلیغات بتواند کارساز باشد. فشارهای عملی در جنگ روانی عبارتند از: ۱) فشارهای اقتصادی ۲) فشارهای نظامی ۳) فشارهای سیاسی – دیپلماتیک ۴) فشارهای فرهنگی –اجتماعی. (اسکندری، ۱۳۸۹ : ۹۶-۹۷)

استاد دانشگاه ملی جنگ امریکا، جان کالینز، جنگ روانی را «استفاده طراحی شده از تبلیغات و ابزارهای مربوط به آن، برای نفوذ در خصوصیات فکری دشمن، با توسل به شیوه‌هایی که موجب پیشرفت مقاصد امنیت ملی شود» تعریف کرده و معتقد است این جنگ انعطاف پذیرترین ابزار برای دستیابی به اهداف است (پیشین ۱۰۲) شیوه‌های جنگ روانی را به طور خلاصه می‌توان چنین بیان نمود: شایعه/ تحریف واقعیات/ اغراق و مبالغه/ تفرقه افکنی/ فریب کاری/ تحریک/ روشنگری و... (برای توضیحات بیشتر ر.ک: منبع پیشین: ۱۰۴-۱۰۸)

۱-۱-۴- عملیات روانی

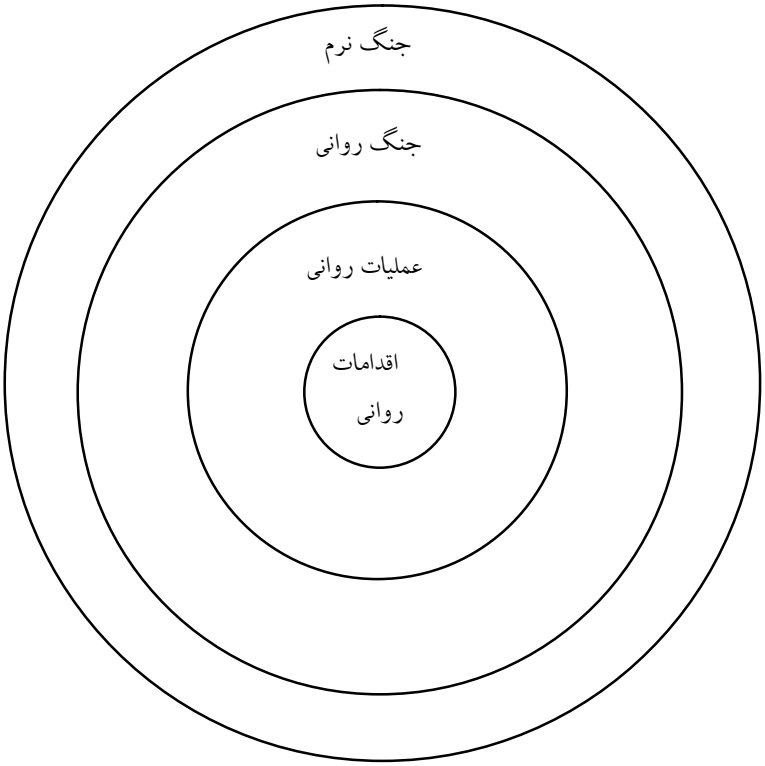
عملیات روانی شیوه‌های موثری است جهت بهره‌برداری از نقاط ضعف روانی نیروهای دشمن با هدف ایجاد ترس، سردرگمی و ناتوانی در آنها که در نهایت تضعیف روحیه طرف مقابل را دربرخواهد داشت. به این ترتیب، عملیات روانی، منطقه نبرد را (بالفعل یا بالقوه) جهت اجرای موفقیت آمیز عملیات، آماده می‌سازد. تاکتیکهای متنوعی در عملیات روانی به کار گرفته می‌شوند که برخی از مهمترین آنها عبارتند از: ارعاب، تهدید یا تشجیع، تطمیع، شستشوی مغزی، فریب، ضدفریب و عملیات امور همگانی. (کمیته پدافند غیرعامل آموزش و پرورش، ۱۲۸:۱۳۸۸) عملیات روانی شاخه‌ای از جنگ روانی است که به منظور تاثیر یا حصول تغییر در برداشتها، عقاید و احساسات فرد یا گروه معین (دوست یا دشمن) در جهت پشتیبانی از اهداف و منافع کشور به کار می‌رود. در فرهنگ وزارت دفاع امریکا عملیات روانی عملیات طرح ریزی شده برای انتقال علایم و اخبار گزینش شده به مخاطبان به منظور تاثیرگذاری بر عواطف، انگیزه‌ها، شیوه استدلال عینی و در نهایت رفتار دولتها، سازمانها، گروه‌ها و افراد بیگانه قلمداد شده است و اصطلاحاً به آن دسته از

اقداماتی گفته می‌شود که به منظور ایجاد تاثیر روانی بر روی فرد یا جامعه مورد نظر به اجرا گذاشته می‌شود تا در نتیجه آن اهداف نهفته در ورای این عملیات تامین گردد. به عبارت دیگر عملیات روانی استفاده حساب شده تبلیغات و شعارها بر ضدحریف در زمان جنگ و یا اعلام وضعیت فوق العاده به منظور پشتیبانی از دستاوردهای کوتاه مدت و بلند مدت ملی است. (اسکندری، ۹۸:۱۳۸۹)

عملیات روانی همراه با تفکر انسان به وجود آمده است. انسانها برای تحت تاثیر قرار دادن مخاطب خود به شیوه‌ها و ترفندهایی متوسل می‌شده‌اند و این فعالیت از ارتباط چهره به چهره دو فرد گرفته تا اجتماعات کوچک و بزرگتری ادامه یافته است و این گونه فعالیتها و اقدامات در زمانهای خاص همچون بحرانها، جنگها، نزاعهای محلی به صورتهای مختلف و گوناگونی اتفاق افتاده است. عملیات روانی، همانند عملیات نظامی سلسله اقداماتی است که برای رسیدن به هدفی خاص و محدود، از نظر زمان و مکان برای غلبه بر حریف انجام می‌شود. تفاوتی که در این دو عملیات وجود دارد یکی در استفاده از ابزاری است که به کار گرفته می‌شوند و دیگر در هدف آنهاست. در عملیات نظامی، از ابزار سخت برای تصرف زمین و جسم انسانها استفاده می‌شود در حالی که شگفت آفرینی عملیات روانی در این است که به کمک ابزار نرم اراده، فکر و روح انسانها به تسخیر درمی‌آید. اقدام روانی فعالیت یا فعالیتهایی است که یک دولت، سازمان، گروه یا به کارگیری شیوه‌های روانشناختی، برای تاثیر گذاشتن بر شرایط سیاسی، اقتصادی، فرهنگی یا نظامی طرف مقابل انجام می‌دهند. گروهی عملیات روانی را استفاده حساب شده تبلیغات و شعارها بر ضدحریف در زمان جنگ یا اعلام وضعیت فوق العاده به منظور پشتیبانی از دستاوردهای کوتاه مدت و بلندمدت ملی دانسته‌اند. حریف، هم می‌تواند به گروه‌های متخاصم اطلاق شود و هم به گروه‌های بی‌طرف یا حتی به گروه‌های خودی (دوست). همچنین از عملیات روانی به عنوان عملیات برنامه ریزی شده برای فرستاد ن اطلاعات و معیارهای گزینش شده به مخاطبان به منظور تحت تاثیر قرار دادن هیجانات، انگیزه‌ها، استدلالهای عینی و رفتار حکومت، سازمانها و یا گروه‌ها به منظور اغوا یا تقویت نگرشها یاد شده است. (اسکندری، ۱۳۸۹ : ۱۰۰–۱۰۲)

از شیوه‌های مرسوم عملیات روانی می‌توان به عملیات روانی سفید، عملیات روانی سیاه، عملیات روانی خاکستری و اقدامات پنهان اشاره نمود. (ن.ک به: منبع پیشین: ۹۹–۱۰۰)

جنگ روانی، عملیات روانی و اقدامات روانی با توجه به ابزار، محیط و زمان تعاریف گوناگونی دارند. اقدامات روانی به فعالیتهایی گفته می‌شود که زیرمجموعه یک یا چند عملیات روانی هستند و عملیات روانی خود زیرمجموعه جنگ روانی است. می‌توان نسبت و رابطه موارد فوق را بدین گونه ترسیم نمود و نشان داد:



شکل ۲: از منظر علم منطق نسبت عموم و خصوص مطلق میان مولفه‌ها و مفاهیم فوق وجود دارند.

۲-۱-۴- بررسی مفهوم کارآمدی و خصلت مشروعیت سازی آن به عنوان سوژه‌ای برای عملیات روانی متخاصمان در عصر جهانی شدن مطالعه موردی

۱-۲-۱-۴- مفاهیم مشروعیت و کارآمدی

از نگاه جوزف فرانکل[1] به گستردگی و شدت پشتیبانی مردم از رهبران «روحیه» اطلاق می‌شود وی اعتقاد دارد که این مفهوم دلالت بر اعتقاد به آینده دولت و درستی اهداف آن داشته بستگی به اوضاع و احوال و کیفیت رهبری دارد و ممکن است دستخوش نوسانهای مکرر و گاه ناگهانی قرار گیرد. (فرانکل، ۱۳۸۳: ۱۶۰) بر این مبنا مشروعیت[2] ویژگی است که قدرت را به اقتدار، یک ناصح یا قدرت را به حاکم سیاسی تبدیل می‌کند و در فقدان آن قدرت به زور محض تبدیل می‌شود. رابرت دال در مورد مشروعیت می‌گوید وقتی

1 - Joseph Frankel
2- Legitimacy

حکومتی مشروعیت دارد که مردم تحت فرمان اعتقاد راستین داشته باشند به این که ساختارها، عملکردها، اقدامات، تصمیمات، سیاستها، مقامات، مدیران یا حکومت از شایستگی، درستکاری یا خیر اخلاقی برخوردار باشند. (دادجو، روزنامه اعتماد: ش ۱۵۷۹) می‌توان گفت بخشی از قدرت در مورد چیزهای مادی است همچون اسلحه، رفاه، انسان، پول، نفت اما قدرت، روحیه[1] را نیز دربرمی‌گیرد. در جهانی که به وسیله شیوع عناصر اغلب مادی پایه ریزی گشته قدرت واقعی که پدیدار می‌گردد ممکن است بنابراین به اعتبار و مشروعیت وابسته باشد. عقیده و وفاداری کوه‌ها را نمی‌تواند حرکت دهد اما می‌تواند انسانها را به تحرک وادارد. از این‌رو اعتقاد بر آن است که هنوز بعدی نهایی از قدرت وجود دارد که نمی‌تواند وانهاده شده باشد: بعد روانشناسانه[2] و همین طور استدلال می‌شود که دو چیز می‌تواند به طور عمده از توانایی هر موجودیت چه دولتی و چه غیردولتی در مورد قدرت متصور بکاهد یا بر آن بیفزاید: ابتدا مشروعیت داشتن در چشمان اعضاء دوم اعتبار آن در چشمان قدرتهای دیگر. (Ferguson, 2003:4)

امروزه در عصر جهانی شدن، ادغام اقتصادها و تکنولوژیها باعث ادغام اطلاعات و ارتباطات گردیده و افزایش اطلاعات مردم باعث پی بردن آنها به حقوق خود و طرح تقاضاهای جدی‌تر شده که در برخی موارد پاسخگویی به آنها خارج از توان حکومتها بوده است. این ناتوانی مشروعیت حکومت را تحت تاثیر قرار داده و آنها را وادار به گزینش می‌کند. گزینه اول تغییرپذیری در داخل حکومتها، ایجاد تغییر در جامعه و در رابطه مردم با حکومت، انتقال تحولات بین المللی به داخل و نیازهای داخلی به خارج است که می‌تواند مشروعیت نظام را حفظ نماید. (فاخری، ۱۲۳:۱۳۸۲) شهروندان به دلیل ویژگیهای جهان در هم تنیده که تبادل داده‌ها و اطلاعات در عمل لحظه‌ای شده است، سطح توقع و انتظار را با شرایط جدید خویش و در مقایسه با شرایط متفاوت و متنوع جهانی تنظیم می‌کنند و خواستار پاسخگویی به این نگاه‌ها و مطالبات‌اند. در واقع تحولاتی که در عرصه مایکروالکترونیک و تکنولوژی اطلاعات رخ داده جهان در حال توسعه را در معرض پدیده‌ای به نام انفجار انتظارات و توقعات قرار داده است. (در این باره ر.ک: مومنی، ۱۳۸۶ : ۱۳۰ و پورپاشا، بی‌تا: ۲۲۲) در واقع بزرگترین تهدید برای حکومتها در دنیای رو به جهانی شدن، عدم توانایی پاسخگویی به انتظارات در حال افزایش مردمی آن هم در شرایطی است که گستردگی و پیچیدگی این مطالبات توان دولتها را در این که خود به تنهایی و بدون حضور مردم، به شناسایی و پاسخگویی آنها بپردازند، به حداقل رسانده است.

1- Morale

2- The Psychological

۲-۲-۱-۴- رابطه کارآمدی و مشروعیت

بین کارآمدی و مشروعیت تعامل و ارتباط دو جانبه و مستمر وجود دارد و به عبارتی هنگامی که پایینیها نخواهند و بالاییها نتوانند سقوط و سرنگونی حتمی است. کارایی با بازده محلی هر سامانه (سیستم) مترادف است و منظور از آن نتیجه بخش بودن یک طرح، برنامه یا سیاست است کارآمدی هم منبع مشروعیت است و هم مشروعیت‌زا و پایه تقویت آن و به نوعی مشروعیت مکمل و ثانویه است. از دید لوسین پای مبنای توسعه سیاسی افزایش ظرفیت سیستمیک و تنوع ساختاری و تخصصی شدن ساختارها در راستای پاسخگویی به خواسته‌های مردم و عبور موفقیت آمیز از بحرانهای شش گانه —بحران هویت، بحران مشروعیت، بحران نفوذ، بحران مشارکت، بحران ادغام، بحران توزیع، در مسیر پیچ و خم توسعه است. (اخوان کاظمی، ۱۳۸۲ : ۸۱-۷۹)

در فرایند جهانی شدن، بازی با حاصل جمع غیرصفر است و کشورها و نهادها و بازیگران سیاسی به طور دائم در کش و قوس، امتیازگیری و امتیازدهی هستند. به تناسبی که مجموعه فعالیتهای یک کشور نمادی از کارآمدی باشد، نهاد دولت در امتیازگیری موفق‌تر است و به تبع آن بهبود وضع رفاهی و ثبات اقتصادی و شهروندان در یک کشور هم اکنون به عنوان مهمترین منبع مشروعیت‌یابی نخبگان سیاسی آن کشور مطرح شده است. هنگامی نیز که تعاریف حکومت کنندگان با تعاریف عامه مردم از اولویتهای ملی تفاوت داشته باشد، شکافهای حاصل از این تعریف باعث بروز بحران مشروعیت و بحران ناکارآمدی می‌شود. (سریع القلم، ۴۹:۸۴) در واقع ناکارآمدی یک حکومت، مقدم و مرجع بر هر چیز دلالت بر «در دسترس نبودن»[1] آن دارد. فلسفه وجودی حکومتها، خاصیت یا استعداد «استفاده شوندگی» (یا در دسترس بودن) آنان است. (تاجیک، ۱۲۴:۸۳) اغلب اذعان شده که هرگاه مجموعه و کلیتی که قرار بود، در نقش کلید و گشاینده‌گره-ها ظاهر شود دچار اخلال در این کار ویژه شود خود به صورت بخشی از مشکل جلوه‌گر می‌شود و این اصل هنگامی که به دولت که وظیفه خطیر آن گشودن گره‌های کلاف سردرگم توسعه و محو سندروم ناپیوستگی توسعه باشد تعمیم یابد ناکارآمدی و در پی آن بحران مشروعیت فرجام کار می‌باشد و در جهان کنونی که امنیت ملی بیش از گذشته به مفهومی چند جانبه بدل گشته در این راستا مفهوم موسع از امنیت تاثیر مستقیمی بر کارایی و افزایش مشروعیت خواهد داشت. امروزه در عصر جهانی شدن سرمنشأ مشروعیت حکومتها کارآمدی آنها قرار گرفته و میزان رضایتمندی شهروندان از خدمات حکومت پشتوانه و عقبه مقبولیت حکومتها بوده و عوامل فرهی و ماوراء الطبیعی نقش کمرنگتری در این زمینه می‌یابند. در ایران با تفاسیری که از مفهوم صدور انقلاب به ویژه در دولت سازندگی به وجود آمد الگو قرار گرفتن کشور در زمینه تحقق اهداف رفاهی و عدالت اجتماعی برای کشورهای منطقه مدنظر بوده که با نیل بدان

1 - Non availability

رسالت صدور انقلاب ایفا گردیده و مدل و نمونه‌ای مترقی و پیشرو ترسیم می‌گشت. به زعم صاحبنظران بحران ناکارآمدی و ناکامی در زمینه تحقق اهداف رفاهی نظام را دچار چالش نموده آفت و نقطه ضعفی برای مدل حکومت دینی بوده و پشتوانه‌های تئوریک آن را در عمل با شکاف روبرو می‌سازد. این امر در دورانی میزان آسیب پذیری را افزایش می‌دهد که هرم سنی جمعیت ایران جوان بوده و در عصر ارتباطات که زمینه‌های مواجهه و مقایسه فراهم می‌شود بحران مشروعیت می‌تواند با شکافها و تقطیعهای اجتماعی و ادغام با بحرانهایی چون بحران جنسی و بحران هویت تبعات امنیتی ناخوشایندی را دربرداشته باشد و دافعه حکومت و نیروی گریز از مرکز آن در برابر شهروندان را پررنگ‌تر بسازد و به عنوان سوژه‌ای برای عملیات روانی دشمنان مورد بهره‌برداری قرار گیرد. در حقیقت این جنگ روانی و عملیات روانی در چارچوب آن یک چرخه و سیکل را باز تولید می‌کند که ابتدا با زمینه‌سازی و مقدمه چینی و هیاهوی جنگ روانی کشور هدف مورد آماج حربه‌ها و تکنیکهای روانی قرار می‌گیرد سپس به عنوان مکمل و عامل تشدید کننده، تحریمها و فشارهای اقتصادی به طرق مختلف بر کشور هدف تحمیل گشته که ضعف اقتصادی و در نتیجه بحران ناکارآمدی و تضعیف دولت هدف اصلی این زنجیره فعالیتهای متخاصمانه می‌شود سپس این ناکارآمدی به صورت یک بحران جلوه داده شده با بزرگنمایی و دامن زدن به آن فاز جدیدی از جنگ روانی آغاز می‌گردد که در نهایت مشروعیت‌زدایی و بحران مشارکت فراگیر کشور هدف را مدنظر دارد. در این چارچوب از هم گسیختگی رابطه دولت و جامعه به عنوان بنیان قدرت دولتها در نظام جهانی به تعبیر کاگلر[1] و دومکه[2] مدنظر است زیرا دولتها از طریق بسیج انسانها و منابع مادی برای عمل ملی دارای ابزارهای نفوذ سیاسی می‌گردند و خدشه در این رابطه و عملکرد تضعیف قدرت و عملکرد ملی را در پی دارد.

خنثی کننده تمامی ترتیبات افندی و بی اثر شدن معادلات متخاصمان در چارچوب جنگ روانی منوط به کارکرد مثبت این فرمول مشروعیت‌زای نظامهای سیاسی است «مسوولان بتوانند؛ مردم بخواهند» هرگونه روند معکوس و اغتشاش در این معادله و فرمول و چارچوب، دشمنان را برای جنگ روانی و سوژه قرار دادن ناکارآمدیها در راستای عملیات روانی خود ترغیب و تحریک و تشجیع می‌سازد تا با باژگونه خوانیها و هیاهو و شانتاژ، راه حلها و روزنه‌ها و کلیدهای حل بحرانها و ستونهای اتکا در نظامات سیاسی را به صورت بخشی از مشکلات و موانع و نقاط ضعف و پاشنه آشیل جلوه داده تصویرسازی منفی و اعتمادزدایی از نظام سیاسی را محقق سازند.

۳-۲-۱-۴- مدل برخورد دشمن در عصر استیلای قدرت هوشمند همگرا

مدل احتمالی برخورد جدید دشمن یک مدل تلفیقی به شکل زیر خواهد بود:

1- Kugler

2- Dumke

۱- تمرکز فشار روانی و سیاسی بر مدیریت سیاسی و دفاعی کشور.
۲- تمرکز فشار عملیات روانی بر مردم و جهان و....
۳- تمرکز فشار عملیات اقتصادی (تحریم)
۴- عملیات نظامی روی اهداف گزینشی و مکمل.
۵- تمرکز تلاشها روی انهدام زیرساختهای حیاتی و حساس مردمی و دفاعی
۶- ایجاد نقاط فوق بحرانی در جمعیتهای عمده مثل تهران و...
۷- هدایت نارضایتی مردم به حوزه اعتراض، اغتشاش و... و در نهایت تخاصم با حکومت
۸- انتقال فشار کمکی نظامی به سمت مقاومتهای باقی مانده...
۹- ایجاد هماهنگی بین پتانسیل تخاصمی مردمی و سیستم تهاجمی نظامی بر حکومت.
۱۰- جابجایی و تغییر سیستم سیاسی و حکومت. (نباتی، ۴۹:۱۳۸۸)

۲-۴- جنگ رسانه‌ای

در دنیای کنونی که سیاستگذاران در پردازش و تدوین راهبردهای خود در سطح بین المللی ایستارهای خود را معطوف به قدرت مضاعف که همان ترکیب قدرت فیزیکی و سخت با قدرت مجازی و رسانه‌ای و انباشت تمامی توانهای پراکنده در محیط قدرت است نموده‌اند شاهد غلبه تصویر و زبان همگانی دیجیتالی در عصر فشردگی زمان – مکان می‌باشیم که به نوعی منطق قدرت را به منطق تکثیر مبدل نموده است و به واقع شاهد آنیم که قدرتهای مجازی و رسانه‌ای جهانی عزمی جدی در انعکاس و نمایش قدرت خویشتن داشته سیستمهای ارزشی خود را در قالب سازه‌های مجازی مفصل بندی نموده برنامه ریزی و سرمایه گذاری عظیمی را در این حوزه برای اعتلا و اشاعه قدرت نرم (که برای پیروزی در دوران به ظاهر صلح ضروری است) و ایجاد جاذبه و هیمنه در عصر تصویرسازی به کار بسته‌اند. در این راستا استفاده از رسانه‌ها برای تضعیف کشور هدف و بهره‌گیری از توان و ظرفیت رسانه‌ها به منظور دفاع از منافع ملی عمومیت یافته است و رسانه‌ها به عنوان یک سلاح برنده و پیش برنده برای تامین منافع له یا علیه هر سیاست اجتماعی به سادگی بسیج شده‌اند و اشکالی از رسانه‌ها همواره در طرحهای استراتژیکی برای هر عملیاتی موضوعیت می‌یابند.

۱-۲-۴- ابزارهای رسانه‌ای

ابزارهای رسانه‌ای همان رسانه‌های مورد استفاده در عملیات روانی جهت انتقال پیام هستند که به پنج دسته عمده شامل تلویزیون (عادی، خبری و ویژه)، رادیو (عادی و ویژه)، خبرگزاریها، مطبوعات (نوشتاری) و اینترنت تقسیم می‌شوند و هر کدام قابلیتهای موثری در امر انتقال پیام دارند و به طور مجزا قادر به اجرای بخشهای تاثیرگذار هستند. این ابزارها به دلیل برد زیاد و فراگیر بودن، در تلقین و القای تحلیلها، اخبار سیاسی و اجتماعی هدفمند بیشترین تاثیرگذاری را بر طرز فکر و اراده مخاطبان دارند. رسانه‌ها با انبوه

اطلاعاتی که انتقال می‌دهند به یکی از ابزارهای شاخص تاثیرگذار بر افکار عمومی تبدیل گشته و پیچیدگی و فراگیر بودن آنها، مقابله با تاثیراتشان را دشوار ساخته است. از این‌رو کشورها به خصوص قدرتهای بزرگ با شناخت این کارکرد و دیگر کارکردهای جذاب رسانه‌ها، در به کارگیری آنها تردید به خود راه نمی‌دهند. (اسکندری، ۱۳۸۹ : ۹۷-۹۸)

در واقع رسانه‌ها با بهره‌گیری از مکانیسمهای کنترل فکری روانی کارکرد خود را که کوچک جلوه دادن بحرانها در جبهه و اردوگاه خودی و بزرگنمایی و آگراندیسمان و اغراق نمایی و دامن زدن به بحرانهای حادث در زمین حریف است با بمباران پیامهای ارتباطی و اخبارهای جهت‌دار و بهره از حربه‌هایی چون باژگونه خوانی حقایق، شانتاژ، مشوه جلوه دادن تصویر حریف، غوغا سالاری و هیاهوگری و مسخ و تحریف و ادغام و جابجایی مرزهای ارزشها و ضدارزشها در منظر و نظرگاه مخاطبان عملی می‌سازند و با هدف برتری جویی نسبت به دشمن یا رقیب خود و تغییر مواضع کشور هدف، استحاله، فروپاشی، براندازی و یا تغییر حکومت مورد نظر را دنبال می‌نمایند.

«نتیجه گیری »

در عصر قدرت هوشمند و قدرت مضاعف اشکال متحول نبرد با بهره از فناوری‌های اطلاعاتی و ارتباطاتی ابزاری است که می‌تواند در نقش آفرینی و قدرت ما نور و میزان قدرت کشورها در عرصه جهانی نقش ایفا نماید.

در این رابطه رویکرد پدافند غیرعامل در نبرد نا متقارن و در وضعیت پدافندی در برابر تکنولوژی‌های برتر و تسلیحات نسل چندم و موضع آفندی و بالادست کشورهای قدرتمند با توجه به تمامی ابزارهای سخت و نرم و تلفیق این دو در تمامی سطوح می‌تواند مورد بهره سیاستگذاران و رهبران قرار گیرد.

شناخت و احاطه بر این فنون،راهکارهایی جهت دفع و خنثی سازی تحرکات دشمنان در دسترس قرار می‌دهد.با توجه به اهمیت جنگ سایبری(رایا نبرد) و فضای مجازی و اولویت و برتری سایبر پولتیک(رایا سیاست) و در کل سیاست ادنی نسبت به سیاست اعلی در عصر کنونی و فضای پس از جنگ سرد اهمیت این مساله بیشتر احساس می‌شود.

کمرنگ سازی عناصری چون کارآمدی و مشروعیت سازی توسط دشمنان که وحدت داخلی کشورها را هدف قرار داده و استحاله درونی و براندازی را جایگزین نبرد مستقیم و فتح قلمرو سرزمینی ساخته و نوعی جنگ نیابتی و غیر مستقیم را در برابر دخالت نظامی به معرض نمایش می‌گذارد، توجه به تمهیدات پدافند غیرعامل را که می‌تواند بدلها و ضد حملات این ترتیبات را ارائه داده و توطئه‌ها را خنثی و بی اثر سازد روزافزون ساخته است.

در این نوشتار سعی بر آن بوده با ترسیم و تعریف مفاهیم و ارائه تصویری از این تمهیدات،راهکارها و

چگونگی ماهیت نبرد در عصر قدرت هوشمند روشن گردد. در این راستا امروزه شاهدیم فضای نبرد از عرصه سرزمینی به فضای مجازی انتقال یافته و مرزها ودیوارهای بتونی و سخت به دیواره‌های آتشین مبدل گردیده و نوعی دگردیسی ماهوی و شکلی را در عرصه نبرد قدرت پدیدار ساخته است.

در نتیجه فضای مجازی باعث بالا بردن سطح مواجهه و مقایسه و اطلاع از جوامع دیگر شده که توقعات و انتظارات شهروندان را شکل می‌دهد، از این رو این فناوری‌ها بسان شمشیری دودم عمل می‌نماید که مقابله با آن‌ها به مدیریت و تدابیری خاص و نا محسوس تا کنترل بی هدف و مستقیم و غیر هوشمند نیاز دارد.

بر این اساس و با توجه به ظهور اشکال جدید اجتماعی جنگ و حیطه‌های جدید نبرد و بازیگران نوین در کنار دولت‌ها ضرورت در پیش گیری فنون نوین در فرایندهای امنیتی،دفاعی و حفاظتی همچون پدافند غیرعامل اطلاعاتی و بهینه سازی سازمان و ساختار دفاعی در راستای دکترین دفاعی در فضای سایبری احساس می‌گردد. بدیهی است پافشاری به در پیش گیری راهبردها و حفظ و استمرار شیوه‌ها و عملکردها و سازمان دفاعی به سیاق سابق و ممانعت از تحول در آنها چه کیفی و چه کمی چه نرم افزاری چه سخت افزاری با توجه به فضای سیال و متحول جهانی سبب ایجاد شکاف‌ها و روزنه‌ها در بدنه دفاعی و ضربه پذیری و تضعیف موازنه قوا می‌شود. لذا در پیش گیری راهبردها و ایستارهای جامع و تکیه بر رویکردهای تلفیقی و فراگیر الزامی است.

در خاتمه می‌توان اشاره نمود در عصر کنونی تمامی ابزارها و کلیه فضاها از پول و تجارت،افراد وشهروندان، ،اسلحه،اتم،لیزر،ماهواره‌ها و رسانه ها،نخبگان،نفت،خدمات دارویی و بهداشتی و.... برای به زانو در آوردن و مطیع ساختن اراده رهبران کشورها مورد بهره برداری و استفاده قرار می‌گیرد تا حتی مزیت‌ها و فرصت‌ها را مبدل به تهدید و نقطه ضعف سازد. در اینجاست که هنر مدیریت در قالب در پیش گرفتن تمهید و رویکرد پدافند غیرعامل می‌تواند مثمر ثمر باشد و حتی نقاط ضعف و محدودیت‌ها را تبدیل به فرصت و نقطه قوت سازد. معنای واقعی قدرت هوشمند نیز در عصر اطلاعات و گسترش فناوری‌های اطلاعاتی و ارتباطاتی و تغییر شیوه‌های نبرد نیز همین گونه می‌باشد.

منابع

«کتب»

۱-اسکندری،حمید (۱۳۸۹) دانستنی‌های پدافند غیرعامل،تهران،بوستان حمید.

۲-تاجیک،محمدرضا (۱۳۸۳) دهه سوم،تخمین‌ها و تدبیرها،تهران،فرهنگ گفتمان.

۳-تلیس،اشلی و دیگران (۱۳۸۳) سنجش قدرت ملی در عصر فراصنعتی،تهران،مو ءسسه ابرار معاصر تهران.

۴- سریع القلم،محمود (۱۳۸۴)ایران و جهانی شدن،تهران،مرکز تحقیقات استراتژیک.

۵-فاخری،مهدی (۱۳۸۲)سازمان جهانی تجارت و سیاست خارجی ج.ا.ا،تهران،دفتر مطالعات سیاسی و بین المللی.

۶-فرانکل،جوزف (۱۳۸۲) روابط بین الملل در جهان متغیر،ترجمه عبدالرحمن عالم،تهران،دفتر مطالعات سیاسی و بین المللی.

۷-کمیته پدافند غیرعامل وزارت آموزش و پرورش (۱۳۸۸) مبانی،اصول و شیوه‌های پدافند غیرعامل،تهران،انتشارات مدرسه.

۸-نباتی،عزت الله (۱۳۸۸) مبانی پدافند غیرعامل،تهران،دانشکده علوم و فنون فارابی.

«مقالات»

۱-آدامز،جیمز (۱۳۸۰) «دفاع مجازی»،ترجمه حسین سلیمی،فصلنامه ی سیاست خارجی،شماره سوم،پاییز ماه.

۲-ابویی،مهدی (۱۳۹۰) «جنگ سایبری و فضای مجازی ایران»،روزنامه شرق،سال نهم،بی جا.

۳-اخوان کاظمی،بهرام (۱۳۸۲) «شاخصه‌ها و شیوه‌های ارتقاء و کارآمدی در نظام ج.ا.ا»،فصلنامه راهبرد،شماره بیست و نهم،پاییز ماه.

۴-پورپاشا کاسین،علی (بی تا) «ایران در راه جهانی شدن:سودها و زیان ها»،اطلاعات سیاسی و اقتصادی،ش ۲۴۱-۲۴۲.

۵-دادجوی توکلی،سپهر (۱۳۸۷)،«انقلاب اطلاعاتی و مفهوم مشروعیت»،روزنامه اعتماد،ش ۱۵۷۹.

۶-دهشیری،محمدرضا (۱۳۸۵) «دیپلماسی غیر دولتی،پیشنهاد یک راهکار جدید برای سیاست خارجی ج.ا.ا»،همشهری دیپلماتیک،شماره هفتم.

۷-شفیعی،حامد (۱۳۹۰) «دکترین فضای سایبری»،روزنامه شرق،سال نهم،شماره۱۳۸۴.

۸-عمیدیان،هاجر (۱۳۹۰) «فضای مجازی بازوی قدرتمند قدرت هوشمند»،همشهری ماه،خردادماه.

۹-مو ءمنی،فرشاد (۱۳۸۶) «چالش‌های اساسی اقتصاد ایران در قرن۲۱»،مجموعه مقالات همایش ایران در قرن۲۱،مو ءسسه تحقیقات و توسعه علوم انسانی.

۱۰-نای،ژوزف.اس (۱۳۹۰) «آینده قدرت»،مهرنامه،شماره۱۴،مردادماه.

«منابع انگلیسی»

1-Ferguson,Nial (2003) What is Power?,Hoover Institution,No2.

2-Ja Ba,Young (2003) Information Technology and The Empowerment of New Actors in International Relations,Journal of International and Area Studies,Volume.10,Number2.