

## تحول در ماهیت جنگ‌های آینده؛ جمهوری اسلامی ایران؛ سناریوها، فرصت‌ها و چالش‌ها

فرزاد رستمی<sup>۱</sup>

تاریخ دریافت مقاله: ۱۳۹۵/۰۶/۱۸

تاریخ تأیید مقاله: ۱۳۹۵/۰۸/۲۷

صفحات مقاله: ۱۹۰ - ۱۴۵

### چکیده:

حیات بشری، مرحله‌ی نوینی از تحولات خود را با ورود به عصر اطلاعات و ارتباطات تجربه می‌کند. حاکمیت عناصر نرم افزاری قدرت و پیشرفت جوامع، تعبیری است که طی دو دهه اخیر بیشتر از هر زمان دیگری مورد توجه بوده است. یکی از مهمترین ابعاد متحول شده در فضای مذکور، مقوله امنیت است. امنیت از دهه ۹۰ تاکنون در بستر چالش‌ها و مسائل نوظهور جهانی، تعریفی نوین و موسع پیدا کرده است. در چارچوب تحولات نرم افزاری امنیت و به تبع آن امنیت بین الملل، مقوله تحول در ماهیت جنگ‌های آینده همواره یکی از مهمترین حوزه‌های مطالعاتی و پژوهشی کارشناسان و پژوهشگران حوزه‌های امنیتی بوده است. پیشرفت‌های چشمگیر در فناوری اطلاعات و ارتباطات بر هدایت، تنظیم و کنترل جنگ‌افزارها و در نهایت نتایج جنگ تأثیرگذار بوده است. در این چارچوب، جمهوری اسلامی ایران از سویی با توجه اینکه دارای ارزش‌ها و هنجارهایی متمایز با ارزش‌های حاکم بر نظام بین الملل است و از دیگر سویی به دلیل اینکه در منطقه‌ای حساس واقع شده که بخش قابل توجهی از رویدادها و روندهای امنیتی جهانی در این منطقه از جهان شکل می‌گیرد، نیازمند بررسی و مطالعه سناریوهای آینده در باب ماهیت جنگ‌هاست. بدون تردید ورود به مباحث جنگ‌ها و منازعات آینده چه در عرصه نظر و چه عمل مستلزم اتخاذ استراتژی کلان و آینده‌نگر است. در این تحقیق ضمن بررسی روندهای امنیتی جهان آینده به ویژه روندهای مربوط به جنگ‌ها بر اساس روش دلفی، به بررسی و شناخت سناریوهای محتمل در این حوزه و در نهایت احصاء چالش‌ها و فرصت‌های فراروی جمهوری اسلامی ایران در باب جنگ‌های آینده پرداخته شده است.

\* \* \* \* \*

## واژگان کلیدی

رونده‌های جهانی امنیت، جنگ، امنیت ملی، ج.ا.ایران، امنیت بین‌الملل، مطالعات آینده، فرصت‌ها/چالش‌ها.

## مقدمه

ورود به عصر اطلاعات و ارتباطات، دربرگیرنده برهه تاریخی حساس دیگری از سیر تطور و تکامل حیات بشری است. ورود به عصر اطلاعات و ارتباطات به عنوان مولفه اساسی پیشرفت کشورها در حوزه‌های مختلف باعث گردیده که شاهد بازتعریف قدرت ملی کشورها در فضای بین‌المللی باشیم. امروزه از قدرت و فناوری و بهره‌مندی از پتانسیل‌های نوین این حوزه به عنوان یک شاخص مهم توسعه در کنار سایر ابعاد قدرت ملی یاد می‌شود. در اینجا مفهوم قدرت ملی دربرگیرنده همه ابعاد اقتصادی، سیاسی، امنیتی، فرهنگی و اجتماعی است. به نظر می‌رسد دسترسی به جدیدترین ابزارهای اطلاعاتی و ارتباطی و بکارگیری دقیق آن در دنیای متلاطم امروزی می‌تواند علاوه بر ارتقاء قدرت سخت کشورها، حوزه‌های تاثیرگذاری قدرت نرم آنان را نیز چندبرابر نماید.

زمانی که ورود به عصر اطلاعات و ارتباطات دربرگیرنده یک جهش علمی و اقتصادی بزرگ برای جامعه جهانی باشد، تسری این حوزه به مباحث امنیتی نیز با توجه به تحولات مهم در ماهیت سیاست و روابط بین‌الملل محتمل می‌نماید. به نظر می‌رسد تحول در مبانی اطلاعات و ارتباطات نقش قابل توجهی در تحولات بنیادین به وجود آمده در ماهیت امنیت بین‌الملل داشته است.

پیچیدگی‌های روز افزون تحولات نظام بین‌الملل و تعاملات تنگاتنگ و نزدیک، فعل و انفعالات سیاسی و فرآیندهای نظامی، محیط جنگهای پیشرفته را از حاکمیت مطلق تاکتیکها و رویه و روشها (استراتژی‌ها) نظامی خارج ساخته و حوزه نفوذ و تاثیر عوامل تکنولوژیکی، اقتصادی، روانی، فرهنگی، سیاسی و... را در این محیط به شدت گسترش داده است. ایجاد اختلال در اطلاعات نظامی دیگران از طریق ابزارهای رایانه‌ای و اینترنت، ایجاد آشفتگی و سردرگمی در فرآیند تصمیم‌گیری گروه‌های هدف، تلاش برای شکل دادن به افکار عمومی جامعه هدف، ایجاد اختلال در تجهیزات راداری، موشکی و پردازش و تحلیل اطلاعات از جمله مصادیق پیشرفت‌های انقلاب اطلاعاتی است که تحت عنوان فرآیندهای جنگ آینده اطلاعات مورد استفاده قرار می‌گیرد. با توجه به اینکه

جمهوری اسلامی ایران نیز طی سال های اخیر تاکید زیادی بر روی قدرت و جنگ نرم داشته و گستردگی دامنه تحولات نرم افزاری امنیت بین الملل را درک کرده، به نظر می رسد ضرورت پرداختن به این موضوع برای ایران دوچندان باشد. بدون تردید ورود به مباحث جنگ های آینده چه در عرصه نظر و چه عمل مستلزم اتخاذ استراتژی کلان و آینده نگر است. هدف از توجه به چنین روندهایی ترسیم چشم انداز امنیتی آینده و برنامه ریزی های استراتژیک برای مقابله با چالش های احتمالی و تقویت نقاط مثبت برای جمهوری اسلامی ایران است. بدون شک کشورهایی که چشم اندازهای آتی خود را ترسیم می کنند توانایی بیشتری برای مقابله با تهدیدها و چالش های فرارو داشته و می توانند به گونه ای بهتر از فرصت های ایجاد شده بهره برداری کنند. بر این اساس و با توجه به اهمیت حوزه مطالعات آینده در جهان معاصر تلاش شده در تحقیق حاضر روندهای آینده پژوهانه امنیت مورد بررسی قرار گرفته و در نهایت سناریوهای مرتبط با حوزه جنگ های آینده که اختصاص به مقوله جنگ های اطلاعاتی به طور خاص دارد، احصاء می گردد. سناریوهای مذکور در چارچوب روش دلفی در مطالعات آینده پژوهی به دست می آید و در نهایت فرصت ها و چالش های احتمالی برای امنیت ملی جمهوری اسلامی ایران مورد بررسی قرار می گیرد.

### چارچوب نظری

یکی از عمده ترین گزاره هایی که در مکتب کپنهاگ، همواره بر آن تاکید می گردد، تحول بنیادین در حوزه های امنیتی است. به این شرح که از اواخر دهه ۸۰ به بعد ماهیت تهدیدات امنیت بین الملل عمدتاً از سخت افزاری به نرم افزاری تغییر جهت می دهد. اگر قبلاً و بر اساس رویکرد رئالیستی حاکم بر روابط بین الملل انباشت سلاح های نظامی و توانمندی در نمایش قدرت نظامی یک کشور تضمین کننده امنیت آن کشور محسوب می گشت، از اواخر دهه ۸۰ مشکلات دیگری در عرصه جهانی ظهور کرد که به نوعی برداشت از امنیت را تغییر داد. (عبداله خانی، ۱۳۸۳: ۱۳۸) از نگاه بری بوزان مهمترین نظریه پرداز مکتب کپنهاگ، امنیت فراتر از بعد نظامی و در بخش هایی چون امنیت اقتصادی، امنیت سیاسی، امنیت فرهنگی و اجتماعی، امنیت زیست محیطی و هم اکنون امنیت اطلاعاتی و سایبری و ... تقسیم بندی می شود. (بوزان، ویور، ۱۳۸۰: ۷۶)

یکی از موضوعات مهمی که در دنیای معاصر روابط بین‌الملل و بر اساس چارچوب نظری مکتب کپنهاک در مقوله تحول در مفاهیم امنیتی قابل بررسی است؛ بحث تحول در ماهیت منازعات و به عبارتی جنگ‌های اطلاعاتی آینده است. اگرچه قبلاً به حداکثر رساندن تسلیحات سخت افزاری نظامی ضامن تامين امنیت یک کشور تلقی می‌گشت، امروز این مسئله در رنگ و لعابی دیگر و در ماهیت جنگ‌های مجازی و سایبری مطرح می‌گردد. بر این اساس امنیت زمانی تحقق می‌یابد که کشورها با استفاده از پیشرفت‌های تکنولوژی اطلاعاتی و کاربردی که این فناوری‌ها در قابلیت‌های جنگی مدرن خواهند داشت، پیروز جنگ در فضای سایبر باشند. البته بیان مباحث فوق به معنای از بین رفتن اهمیت تسلیحات سخت افزاری نظامی در دنیای امروز نمی‌باشد بلکه به معنای اهمیت روز افزون مقوله جنگ‌های اطلاعاتی در آینده است.

در چارچوب اهمیت سطح مناسبات امنیت سایبری در منازعات آینده کشورها با هدف ارتقاء سطح امنیت ملی خود به این سمت خواهند رفت که از تاکتیک‌های جنگی غیرمعمول به عنوان راهکار جنگی در مواجهه با نیروهای نظامی پیشرفته استفاده نمایند. تکنولوژی‌هایی همچون ماهواره، اینترنت، تلفن همراه و سایر سیستم‌های اطلاعاتی با قابلیت‌های بالا که می‌توانند حجم قابل توجهی از اطلاعات را ذخیره و انتقال دهند به شکل گسترده‌ای می‌توانند عملیات‌های جنگی مخربی را در فضای سایبر بر علیه کشور هدف سازماندهی نمایند. این مسئله هم اکنون به یکی از حوزه‌های تقابل چالش برانگیز چین و آمریکا در فضای سایبر تبدیل شده است. بر اساس شکل‌گیری چنین روندهایی است که موسسات فعال در حوزه مطالعات آینده پیش‌بینی می‌کنند که تا سال ۲۰۲۵ برخی از کشورها احتمالاً از سلاح‌هایی استفاده می‌کنند که جهت تخریب و نابودی سیستم‌ها و شبکه‌های اطلاعاتی، حس‌گرها و سیستم‌های ارتباطی طراحی شده‌اند، مثل سلاح‌های ضد ماهواره، ضد رادیو فرکانس و سلاح‌های لیزری. مباحث مذکور که از سویی در چارچوب تفسیر موسع از مباحث امنیتی ارائه می‌گردد و از سوی دیگر حاکی از تغییرات بنیادین در مقوله امنیت سخت افزاری است، در چارچوب تحلیلی مکتب کپنهاک قابل توجیه و تبیین است. دامنه تحولات مذکور در بخش سناریوهای تحقیق حاضر مورد بررسی قرار می‌گیرد.

## مروری بر تاریخچه جنگ‌ها

جنگ به عنوان پدیده‌ای اجتماعی، مفهومی ناشناخته است و برای آن تعریف و گزینه‌های مختلف و متنوعی ارائه شده است. هر اندیشمند و صاحب نظری در علوم سیاسی، نظامی، اجتماعی، جامعه‌شناختی و ... بر پایه بینش و گرایش از دیدگاه مطالعاتی خود، جنگ را به گونه‌ای تعریف و تبیین کرده است. (قاسمی، ۱۳۸۷: ۵۱) تحولات جنگ از پدیده‌های تلخ ولی واقعی زندگی بشری است. انسان‌ها به منظور تحمیل اراده خود به دیگری، از آن استفاده می‌کنند. با این حال به سختی می‌توان جنگ را تعریف کرد؛ اگرچه بر سر این نکته اتفاق نظر وجود دارد که جنگ، خشونت نظامی سازمان یافته است، اما نمی‌توان به درستی دریافت که چه میزان خشونت را می‌توان جنگ نامید. کلاوزویتس از مشهورترین نظریه پردازان نظامی غرب، جنگ را عمل خشونت آمیزی تعریف می‌کند که منظور از آن، واداشتن شخص به پذیرش و اجرای اراده ماست. (Clausewitz, 1957: 23-24)

با توجه به اینکه در قرون وسطی، انحصار قدرت و قوه قهریه در دست کلیسا بود، آنها «کنستانتین» را که در پیشاپیش خود صلیب حمل می‌کرد، سرمشق قرار داده و آرمان‌های دین و جنگ را با یکدیگر ادغام کردند؛ شاید بتوان گفت که در این دوران، حداقل در اروپا، این باور غالب وجود داشت که «جنگ ادامه مذهب است» و جنگ‌های سبعانه‌ای را که در تاریخ نظیر نداشت، به وقوع پیوست. این دوران تا اواخر قرن هفدهم میلادی ادامه داشت. پس از آن جنگ‌های کوچک و بزرگ فراوانی توسط دولت-شهرها به راه انداخته شد و دامنه آن سراسر اروپا را فراگرفت که از آن به عنوان «جنگ همه علیه همه» یاد می‌شود. در همین فاصله مطابق قرارداد وستفالی، دولت‌های بزرگ در اروپا شکل گرفت و سه مفهوم دولت، ملت و ارتش ظهور یافته و پایه و محور اساسی نظریه‌های جنگی شد. در این دوران، انحصار استفاده از قدرت، در اختیار دولت‌های بزرگ قرار گرفت. در همین مقطع بود که کلاوزویتس نظریه خود را مطرح ساخت و اظهار داشت: «جنگ توسط کشورها انجام می‌شود و ادامه سیاست دولت‌ها است». (محمدی، ۱۳۸۸: ۴۵-۴۴) بنابراین دولت‌ها حق انحصاری جنگ را به دست گرفتند؛ اما با پیشرفت‌های فناورانه و انقلاب در ارتباطات و اطلاعات در دوران معاصر، گروه‌ها و افراد دیگری چون شبه نظامیان، مزدوران، جنگ سالاران و ... وارد عرصه جنگ شدند و

انحصار جنگ را از دست دولت‌ها خارج ساختند. این اندیشه جدیدی نیست که، «هر تمدن راه خاص خود را برای برپاکردن جنگ پدید می‌آورد» خود کلاوزویتس به این نکته اشاره می‌نماید که: «هر عصری شیوه جنگی عجیب و مخصوص خود را داشته است؛ بنابراین در هر عصری شاهد شکل‌گیری نظریه‌ای در باب جنگ متناسب با آن دوره زمانی و تحولات محیطی خواهیم بود. (همان، ۴۶-۴۴)

### جنگ‌های سستی و نوین

امروز به جز تعداد معدودی از جنگ‌ها که بر اساس الگوی جنگ‌های سستی به وقوع می‌پیوندند، بیشتر جنگ‌های عصر ما از این الگو پیروی نمی‌کنند و تعریفی که کلاوزویتس از جنگ ارائه نموده امروز کمتر در مابانی و مولفه‌های اساسی جنگ‌های نوین دیده می‌شود. (مارتین فن، ۱۳۸۶: ۱۱-۵) در این رابطه و در ابتدا باید گفت که بخش اعظم جنگ‌هایی که به شکل جدیدتر انجام می‌شوند فاقد علامت مشخصه بین دولت‌ها یعنی نبرد سرنوشت‌ساز هستند. در جنگ بین دولت‌ها طرف‌های درگیر در جنگ، همه توان و نیروهای خود را در مکان و زمانی مناسب جمع می‌کردند و به طور کلی همه لشکریان در یک محل مستقر می‌شدند و قوای خود را بر ضد دشمن متمرکز می‌کردند و در مکان و زمان خاص با دشمن وارد جنگ می‌شدند. در جنگ‌های سستی دو طرف درگیر در جنگ سعی داشتند تا تصمیم‌نهایی درباره اختلاف خود را به نبردی محول کنند که نتیجه آن به عنوان مبنا و چارچوب تعیین‌کننده‌ای برای مذاکرات صلح آینده باشد. از ویژگی‌های دیگر جنگ‌های سستی می‌توان به در نظر گرفتن آغاز و پایانی مشخص برای آن اشاره کرد به طوری که طبق قواعد خاص اعلان جنگ صورت می‌گرفت و بر طبق همین قواعد اولیه، جنگ خاتمه می‌یافت و اینکه، این جنگ از نظر زمانی، کوتاه مدت و محدود بود. (مونکلر هرفرید، ۱۳۸۶: ۱۶-۱۴) به طور کلی می‌توان گفت که جنگ سستی جنگی است که بوسیله نیروی نظامی یونیفورم پوش صورت می‌گرفت که رویارویی قطعی در جبهه نبرد بود. (همان: ۱۵) بر خلاف نیروهای ارتش حرفه‌ای، امروزه مجموعه‌ای از بازیگران و شبکه‌های دولتی، بازیگران غیر دولتی، عملیات چریکی و نامتقارن، جنگ‌های اطلاعاتی و ... وارد فضای جنگ‌های سستی شده و به آن شکل می‌دهند. از دیگر تفاوت‌های عمده جنگ‌های سستی و نوین این است که امروز و

در جنگ‌های نوین، دولت، انحصار خود در جنگ را از دست داده است که واضح ترین شکل آن، ظهور هر چه بیشتر بازیگران شبه دولتی مخصوص است که با تجاری شدن نیروهای جنگی و مخدوش شدن فزاینده مرز میان استفاده از خشونت در زندگی روزمره، شتاب می گیرد. نزاع ها و برخوردهای سستی برون مرزی بین دولت ها هر چه بیشتر جای خود را به ستیزه جویی های درون مرزی می دهد. در رواندا، یوگسلاوی، چین و افغانستان بررسی ها شاهد ظهور بازیگرانی جدید با اهداف و مقاصد جدید در میدان منازعه هستند. موضوع دیگر که به دنبال تفاوت های مذکور میان جنگ‌های سستی و نوین وجود دارد، جنگ ناهمگون است. اگر چه جنگ ناهمگون از زمان طرح نخستین جنگ‌ها، مطرح بوده است اما آنچه باعث تمایز جنگ‌های ناهمگون معاصر از نوع سستی آنها می شود، یک بهره گیری از سامانه‌های ارتباطی و نیز برخورداری گروه‌ها و شبه نظامیان از ابزارهای توانمند نظامی و دیگری مطرح شدن جنگ ناهمگون به عنوان یک راهبرد و نه تاکتیک برای جنگیدن است. در سالهای اخیر جنگ ناهمگون بیش از پیش در کانون توجه قرار گرفته است و بسیاری از مباحث جاری در حوزه نظامی، از این مقوله است. جنگ ناهمگون با افزایش نگرانی دشمن از احتمال تحول حملات مرگبار و همراه با خشونت زیاد نه تنها مقدمات روانی ناهمگون سازی را در سیر ابعاد نبرد فراهم می کند، بلکه ظرفیت های ذاتی موفقیت و شکست دشمن را ارتقاء می بخشد. آمریکایی ها برای اولین بار در ویتنام تجربه کردند که تشکیلات نظامی در برابر راهبردهای ناهمگون چقدر بی دفاع است زیرا با وجود برتری، آنها از نظر تسلیحاتی نتوانستند دشمنانی را که از هر نظر ضعیف بودن را شکست دهند. آسیب پذیری شدید آمریکا در لبنان و سومالی زمانی بیشتر روشن شد که پایگاه نیروی دریایی آمریکا در بیروت با بمب مورد حمله قرار گرفت. (همان: ۴۹-۵۰)

ضربه پذیری در جنگ‌های ناهمگون زمانی بیشتر می شود که جنگ به سایر حوزه‌ها هم کشیده شده و با ابزارهای دیگر انجام شود. در این مرحله است که ضرورت توجه به اهمیت رسانه‌ها در جنگ مشخص می شود. ظهور جنگ در رسانه‌ها مهمتر از هدف های درگیر جنگ است. تلاش رسانه‌ها همسو با گردانندگان و سیاست گذاران عرصه دیپلماسی یک کشور در جهت شکل دهی به افکار عمومی با استفاده از ابزار تبلیغاتی است. (همان: ۵۱-۵۲) به قول بودریار در اینجا طرح مفهوم واقعی بیشتر از خود واقعیت واقعی است. یعنی بیشتر از آنکه اصل موضوع و رخداد مهم باشد،

تفاوت در نوع پوشش و بازنمایی خبری می‌تواند مهم باشد. استفاده از تصاویر، نشانه، نمادها و ... می‌تواند زمینه دیگری از ناهمگون سازی جنگ‌ها در فضای نوین منازعات باشد. (ژان بودریار، ۱۳۸۰: ۱۶-۱۴) موضوعی که در مباحث آینده تحت عنوان انقلاب اطلاعات و ابعاد مختلف آن مورد بررسی قرار خواهد گرفت در واقع ترتیبات جدید تری را از تحولات جدید جنگ در دنیای معاصر و آینده منازعات را به تصویر می‌کشد.

### جنگ اطلاعات

در طول تاریخ، جنگ به انواع گوناگونی دسته‌بندی و طبقه‌بندی شده است. انواع جنگ و ترکیب دیگر مفاهیم با آن، برای خلق یا تعریف پدیده‌ای جدید در عرصه منازعات انسانی، چنان گسترش یافته است که رسیدن به دریافتی مناسب از همه آنها بر اساس تنها یک نگرش خاص یا یک زاویه دید معین، بعید به نظر می‌رسد. از سوی دیگر روند رو به رشد تولید مفاهیم نو در عرصه موضوعات مربوط به جنگ آینده نیز دشواری دستیابی به درکی به نسبت جامع از انواع جنگ را دو چندان کرده است. با این حال، ملل جهان بر اساس فرهنگ، تجربه‌ها، شرایط، مقدرات و در راستای اهداف و مقاصد خود، انواع جنگ را طبقه‌بندی کرده‌اند. عناصر پیش‌گفته در طبقه‌بندی انواع جنگ و تأکید بر نوع خاصی از جنگ سهم بسزایی دارد. (ادوارد والتس، ۱۳۸۶: ۱۵۲-۱۴۷)

در طول تاریخ، کسب پیروزی‌های بزرگ نظامی در اغلب مواقع مرهون برتری در زمینه‌ی تحرک، قدرت آتش، اطلاعات یا لجستیک قلمداد می‌شده و سیستم‌های برتر فرماندهی و کنترل، فرماندهان را قادر می‌ساخته تا با حفظ انسجام اقدامات صورت گرفته، این قابلیت‌ها را در زمان و مکان مقتضی به کار بسته، به پیروزی دست یابند. پیچیدگی‌های روز افزون تحولات نظام بین‌الملل و تعاملات تنگاتنگ و نزدیک، فعل و انفعالات سیاسی و فرآیند‌های نظامی، محیط جنگ‌های پیشرفته را از حاکمیت مطلق تاکتیکها و رویه و روشها (استراتژی‌ها) نظامی خارج ساخته و حوزه نفوذ و تاثیر عوامل تکنولوژیکی، اقتصادی، روانی، فرهنگی، سیاسی و... را در این محیط به شدت گسترش داده است. (Mishear R.C, 2003:58)



بر این اساس مفهوم جنگ اطلاعات در چارچوب نظام‌مند امروزمند خود در سال ۱۹۷۵ میلادی مورد استفاده قرار گرفت و در سال‌های میانی دهه ۹۰، وارد ادبیات نظامی امنیتی شد. از زمان جنگ دوم خلیج فارس، تحلیلگران نظامی تغییرات قابل ملاحظه‌ای را در جنگ‌های نظامی پیش‌بینی کرده‌اند. این تغییرات به صورت گذار از تخریب گسترده فیزیکی به حمله دقیق و حتی تخریب غیرفیزیکی در قالب جنگ اطلاعات ترسیم شده است. تاکنون، تعریف‌های گوناگونی برای این نوع تخصصی جنگ ارایه شده است. برخی از تعریف‌های ارایه شده به حدی گسترده بوده‌اند که نمی‌توان حدود معینی را برای آنها متصور شد. برای مثال، توماس رونا، یکی از ترویج‌کنندگان اولیه جنگ اطلاعات، تعریف زیر را که تعریف بسیار گسترده‌ای است، ارایه کرده است:

«رقابت‌های تاکتیکی، عملیاتی، استراتژیکی در کل طیف صلح، بحران، افزایش بحران، درگیری، جنگ، خاتمه جنگ و مقاطع بازگشت به وضعیت ثبات بین رقباء، متخاصمان یا دشمنان که با استفاده از شیوه‌ها و ابزار اطلاعاتی برای دستیابی به اهداف صورت می‌گیرد».

تعریف دیگری که در این زمینه ارایه شده است و بیشتر جوامع نظامی و امنیتی از آن استفاده می‌کنند عبارت است از:

«مجموعه اقداماتی که برای تأثیرگذاری بر اطلاعات و سیستم‌های اطلاعاتی دشمن صورت می‌گیرد و در عین حال، از اطلاعات و سیستم‌های اطلاعات خودی محافظت می‌کند»

(Greg Rattary, 2001:66)

- نقش و تأثیرگذاری مقوله اطلاعات در جنگ در سه حوزه قابل بررسی می‌باشد:
- فن‌آوری اطلاعات و ارتباطات موجب گسترش دامنه حفاظت و شناسایی دید و هدف یابی دشمن شده و میزان برد درگیری را ارتقا، بخشیده است.
  - دوم، اهمیت و نقش فن‌آوری پردازش و ارتباطات افزایش یافته و باعث افزایش سرعت دسترسی فرماندهان به اطلاعات حساس در جنگ شده است.

▪ به کارگیری فن‌آوری اطلاعات در تسلیحات نیز موضوع سوم و قابل بررسی در این حوزه است که باعث افزایش سطح دقت پرتاب شده و موجب ارتقاء سطح قدرت کشتندگی در این سلاح‌ها شده است. (Leigh Armistead, 2007:54-58)

به طور کلی جنگ اطلاعاتی عبارت است از: استفاده از شبکه‌های الکترونیکی برای تخریب یا از کار انداختن و غیر عملیاتی کردن زیرساخت‌های اطلاعاتی دشمن که هم می‌تواند علیه یک جامعه و هم علیه ارتش یا نیروی نظامی یک کشور به کار گرفته شود.

### ویژگی‌های جنگ اطلاعات

به طور کلی می‌توان شش ویژگی اصلی را برای جنگ اطلاعات برشمرد که به اختصار مورد بررسی قرار می‌گیرد:

### گسترده‌گی

این مشخصه دربرگیرنده میزان شعاع اثر عملیات است. عملیات‌های اطلاعاتی بیشترین شعاع اثر را در میان انواع مختلف عملیات‌ها به خود اختصاص داده‌اند و تسلیحات اطلاعاتی نیز بیشترین شعاع اثر را در میان انواع تسلیحات دارند. به عنوان مثال در حالی که بیشترین شعاع اثر تسلیحات حیظه‌های دیگر نبرد به سلاح اتمی با شعاع اثر بیشینه چند صد کیلومتر مربع تعلق دارد، شعاع اثر یک سلاح اطلاعاتی نظیر تبلیغات می‌تواند بالغ بر میلیون‌ها کیلومتر مربع باشد. (فناوری و قدرت ملی چالش‌ها و راهبردها، ۱۳۸۸: ۳۷۱-۳۷۲)

### همه‌جانبه‌گرایی

همه‌جانبه‌گرایی به این معنی است که طیف متنوعی از اهداف، خواسته یا ناخواسته مورد اصابت سلاح اطلاعاتی قرار گیرند. به عنوان مثال در حالی که سلاح اتمی با داشتن بیشترین عمق اثر در میان تسلیحات حیظه‌های دیگر نبرد می‌تواند مردم و تاسیسات فیزیکی یک محدوده را تحت تاثیر قرار دهد اما سلاح اطلاعاتی تبلیغات می‌تواند در کمترین زمان سیاستمداران، رهبران، فرماندهان نظامی و مردم را تحت تاثیر قرار دهد. (همان: ۳۷۲-۳۷۳)

### کیفی بودن

ماهیت کیفی تسلیحات اطلاعاتی است که ویژگی های گستردگی و همه جانبه گرایي را در جنگ اطلاعات قابل توجه و قابل پذیرش می نماید. به عنوان مثال تصمیم گیری، تفکر یا آگاهی مولفه‌هایی کیفی هستند که اطلاعات آنها موثر است. بنابراین هدف گیری آنها یک عملیات کیفی محسوب می شود. کیفی بودن جنگ ماهیت آسیب شناسانه خاصی به این مدل جنگ می بخشد چرا که محاسبه آسیب های کیفی وارد آمده به یک سیستم همواره مشکلات غیرقابل پیش بینی ای را به دنبال خواهد داشت. (Rafael Gaspar, 2003:346-382)

### اخلال‌گری

اخلال‌گری به عنوان اصلی ترین اثر جنگ اطلاعات محسوب می شود. اثر اخلال‌گری توجیه کننده چرایی گسترش و همه جانبه گرایي جنگ اطلاعات و نتیجه طبیعی کیفی بودن این نوع جنگ است. ویژگی قابل توجه دیگر اثر اخلال، کاهش تلفات فیزیکی و به عبارت دیگر تلفات کمی است. در حالی که تلفات کیفی به مراتب اثرگذاری مخرب تر و طولانی تری از خود به جای می گذارند. (روزنا، ۱۳۸۹: ۹۱-۹۶)

### عدم تقارن

در صورت حمله اطلاعاتی به کشوری که از قدرت نظامی محاسبه شده و مشخصی برخوردار است نمی توان انتظار داشت پاسخ حمله، نسبتی منطقی از توان نظامی آن کشور باشد. به طوری که حتی احتمال چندین برابر شدن شدت عکس العمل کشور مزبور که در محاسبات معمول قابل تعریف نبوده است نیز وجود دارد. از این رو عدم تناسب عکس العمل هدف به قدرت حمله، ایجاد کننده نوعی عدم تقارن است. عدم تناسب در جنگ اطلاعات که منجر به نامتقارن شدن این جنگ می شود می تواند ناشی از دلایل گوناگونی باشد از جمله: بهره مند نبودن حمله کننده از منابع اطلاعاتی مشابهی که خود آنها را مورد حمله قرار داده است، عدم توان کافی مدافع در واکنش متناسب اطلاعاتی به دلیل محروم بودن از سلاح اطلاعاتی مناسب، ناشناس بودن مهاجم، اهداف و ماهیت حمله، اندک بودن هزینه

عملیاتی به نسبت اثر وارده، عدم تمایز دقیق میان عملیات جنگ و فعالیت جنایتکارانه و ... (فناوری و قدرت ملی، ۱۳۸۸: ۳۷۵)

### سرعت محوری

شاخص زمان یا سرعت همواره از اهمیت ویژه‌ای در میان تئوریسین‌های نظامی برخوردار بوده است. از مقطع معرفی تسلیحات اتمی و مدل جنگ‌های اتمی این بحث اهمیت بیشتری پیدا کرد. طوری که بسیاری مولفه اصلی پیروزی در جنگ اتمی را برتری در شاخص زمان می‌دانستند. هم‌اکنون و در مقطعی جدیدتر و معرفی جنگ اطلاعات، یک بار دیگر تحول جدیدی در تاثیرگذاری شاخص زمان در جنگ‌های مدرن رخ داده است. سرعت به عنوان یکی از ویژگی‌های اساسی جنگ اطلاعات به دو گونه عملیات‌های اطلاعاتی را تحت تاثیر قرار می‌دهد. نخست از طریق افزایش سرعت خبرگیری و پردازش و محاسبه اطلاعات نیروهای خودی و در نتیجه کاهش دادن زمان تصمیم‌گیری و دوم لخت کردن سیستم نظامی دشمن از طریق کاهش سرعت خبرگیری و پردازش و تصمیم‌گیری او. (همان: ۳۷۷)

### انواع جنگ اطلاعات

جنگ اطلاعات دربرگیرنده انواع مختلفی از جنگ‌هاست. این نوع جنگ‌ها یا به تعبیری راهبردها، زیرمجموعه جنگ اطلاعاتی تلقی می‌شوند و هر یک در مقاطع زمانی مختلف و با توجه به امکانات و شرایط، اولویت بیشتری را در بر می‌گیرند. جنگ‌های اطلاعات اگرچه انواع مختلف دارند اما در اینجا به دلیل اهمیت آنها و ارتباط معنایی آنها به چهار نوع از این جنگ‌ها اشاره می‌گردد:

### جنگ الکترونیک<sup>۱</sup>

جنگ الکترونیک یکی از اشکال جنگ اطلاعات محسوب می‌شود که دربرگیرنده دامنه وسیعی از اقدامات مرتبط با حوزه ارتباطات است که با استفاده از امواج الکترونیکی و رمز صورت گرفته، ضامن تسهیل در دریافت اطلاعات مطمئن برای نیروهای خودی و کاهش ضریب اطمینان دریافت اطلاعات

۱ - Electronic Warfare

مطمئن و به هنگام برای نیروهای دشمن است. عمده اقدامات ضد رادار، ضد رمز و ضد ارتباطات در این چارچوب قرار می گیرد.

اهداف جنگ الکترونیک به عنوان زیرمجموعه ی از جنگ اطلاعات را می توان به ۳ بخش عمده زیر تقسیم کرد:

- سیستم های ضد رادار: در این بخش از جنگ های الکترونیک، به کار انداختن یا به اشتباه انداختن سیستم های راداری دشمن هدف غایی به شمار می آید.
- سیستم های ضد ارتباطات و مخابرات: در این بخش سیستم های مخابراتی و ارتباطاتی دشمن مورد هدف قرار می گیرد.
- رمزنگاری: این مفهوم تحت عنوان رمزنگاری در جنگ الکترونیک از اهمیت بسزایی برخوردار است. هدف از کد کردن سیگنال های الکترونیکی این است که در صورتی که دشمن بتواند این سیگنال ها را بشنود یا دریافت کند، قادر به احصاء مفهوم سیگنال ها نشود. (cordesman,2002)

### جنگ سایبری<sup>۱</sup>

جنگ سایبری یکی دیگر از انواع جنگ اطلاعاتی محسوب می گردد که در فضای سایبر در می گیرد. فضای سایبر اصطلاحی است که بیشتر در هم تنیدگی شبکه های ارتباطی، پایگاه ها و منافع اطلاعاتی را نشان می دهد. که دربرگیرنده پوشش های متنوع، مختلف و گسترده مبادلات الکترونیکی است. نظریه پردازان پیشگام جنگ اطلاعات یعنی جان آرکویلا و دیوید راند فلت بر این باورند که در هر جایی که سیستم تلفن، کابل کواکسیال، خط فیبر نوری یا امواج الکترونیکی وجود دارد، فضای سایبر نیز وجود داشته و از اهمیت ویژه ای برخوردار است. این نوع مقابله و جنگیدن ابعاد مختلفی را در برمی گیرد از جمله: خرابکاری اینترنتی، جمع آوری داده ها با هدف دسترسی به اطلاعات طبقه بندی شده، ایجاد اختلال در سرویس دهی، ایجاد تغییر و اختلال در تجهیزات ارتباطاتی و ماهواره ای و حمله به زیرساخت های حیاتی

---

۱ - Cyber Warfare

یک کشور مثل تاسیسات سوخت رسانی، نیروگاه‌های برق، ارتباطات و حمل و نقل و ... (John, Peterson, 1996: 99-101) این شکل از جنگ اطلاعات همچنین دربرگیرنده طیف وسیعی از تروریسم اطلاعاتی<sup>۱</sup>، حملات معنایی<sup>۲</sup>، جنگ شبیه سازی<sup>۳</sup> و ... (Anthony H. Co desman, 2002: 96-105)

### جنگ C41<sup>۴</sup>

جدا ساختن مسیر ساختار فرماندهی دشمن از بدنه نیروهای تحت فرمان، هدف اساسی این نوع از جنگ‌های اطلاعاتی محسوب می‌شود. این نوع از جنگ‌ها دربرگیرنده دو بعد اصلی می‌باشد:

#### الف) عملیات ضد سر<sup>۵</sup>

این نوع عملیات درگذشته بر حذف فیزیکی فرماندهان عالی جنگ متمرکز بوده است و به طور کلی حذف آنها تاثیرات قابل توجهی بر نتایج جنگ داشته است. مراکز فرماندهی زمان ما، با ارتباطات زیاد و محسوس و درگیر بودن رایانه ای و الکترومغناطیسی و رفتارهای متمایز که این محل‌ها را از سایر محل‌های نظامی متمایز می‌کنند تشخیص داده می‌شوند. حمله به یک مرکز فرماندهی به ویژه اگر به موقع انجام گیرد، می‌تواند حتی بدون ضربه زدن به یک فرمانده عالی رتبه دشمن، موجب مختل شدن حوزه و گسترش عملیات گردد.

در این میان مثل گذشته تنها راه حمله به مراکز فرماندهی استفاده از بمب‌های فلزی نیست، بلکه می‌توان با قطع برق، استفاده از دخالت الکترومغناطیسی و وارد کردن ویروس رایانه ای سیستم‌ها را مختل کرده و یا به کلی از کار انداخت. (فناوری و قدرت ملی، ۱۳۸۸: ۹۲)

۱ - Information Terrorism

۲ - Information Terrorism

۳ - Simulation-Warfare

۴ - Command Control, Computer and Communication Warfare

۵ - Antihead

## ب) عملیات ضد گردن

این نوع عملیات خطوط ارتباطی و اطلاعاتی فرماندهی و بخش های مختلف صحنه عملیات را هدف قرار می دهد و هدف آن ارتباطات الکترونیکی صحنه عملیات است. سازمان ها و رده های مختلف ارتش های مدرن از اواسط قرن نوزدهم به وسیله ارتباطات الکترونیکی و از دهه بیست با مخابرات رادیوالکترونیکی به هم مرتبط شده اند، اگر این ارتباطات قطع گردد، موجبات فلج شدن فرماندهی و کنترل فراهم می گردد. در این نوع از عملیات ها، اینکه یک کشوری تا چه اندازه در سیستم های رایانه ای پیشرفت داشته باشد، در اثرگذاری جهت حملات تعیین کننده است. یک شبکه رایانه ای مرکب از تعداد زیادی رایانه های کوچک، هم امواج کمتری منتشر می کند و هم اینکه سایه کوچکتری می اندازد.

### جنگ روانی<sup>۱</sup>

استراتژیست ها و کارشناسان جنگ اطلاعات، یکی از مهمترین فاکتورهای اساسی موفقیت در جنگ را جنگ روانی می دانند. از نگاه کارشناسان این حوزه، در اینجا دیگر پیروزی در هر جنگ و شکست دشمن معیار نیست، بلکه کسی موفق است که بدون شرکت در جنگ و بدون صرف هزینه های سرسام آور نظامی و سخت افزاری بتواند دشمن را شکست دهد. (همان: ۱۰۸) هر چه از جنگ های سستی به سمت جنگ های مدرن حرکت کنیم، نقش عملیات روانی در جنگ های مدرن رو به گسترش است. امروزه از آن با عناوین مختلفی نام می برند. فولر در سال ۱۹۲۰ اصطلاح جنگ روانی را برای بعد روانی جنگ به کار برد و معتقد بود کم کم مسائل سستی جنگ ها جای خود را به جنگ های روانی که در آنها از سلاح کمتر استفاده می شود، می دهد. اهداف جنگ روانی عبارت است از: زایل کردن خرد انسانی و حیات معنوی و اخلاقی یک ملت از طریق نفوذ در اراده آنها. بعد از جنگ، اصطلاح جنگ روانی، به واژه جدید عملیات روانی و اقدامات روانی تغییر یافت و هدف از آن اقدامات سیاسی، نظامی، اقتصادی و ایدئولوژیکی بود که برای ایجاد احساسات، نگرش ها، رفتارهای مطلوب در گروه های دوست، دشمن، بی طرف و مخالف، به منظور تامین مقاصد ملی، طراحی و اجرا می شد و سپس به یکی از ۴ عناصر اصلی قدرت در نظام های بین الملل تبدیل و به رسمیت شناخته شد و در عالی ترین سطوح دولتی، نظامی و بین المللی، همواره با

۱ - Psychological Warfare

عوامل سیاسی، اقتصادی و نظامی در تصمیم‌گیری‌های عمده سیاست خارجی دولت‌ها، نقش عمده‌ای ایفا کرد که البته با پیشرفت‌های فناوری در علم ارتباطات و رسانه نیز شکل جدی‌تری یافت و نقش آن را در مرتبه‌ی عالی‌تری قرار داد.

بر این اساس امروزه جنگ روانی کارآمدترین و به صرفه‌ترین ابزار جنگ بر ضد نیروهای دشمن محسوب می‌شود. به طور کلی اهداف جنگ روانی در محورهایی همچون؛ تلاش در جهت تخریب فرهنگ و ایدئولوژی یک ملت، اقدام بر ضد باورهای ملی دشمن، تخریب مقبولیت رهبران دشمن، توسل به اقدامات روانی بر ضد نیروهای درگیر خارجی از طریق نمایش عمومی و قدرت در میان آنها به وسیله مانورهای تبلیغاتی مختلف قابل بررسی است. (Emily O. Goldman, 2003: 57-62)

### قدرت‌های بزرگ و جنگ اطلاعات

#### ایالات متحده آمریکا

به دلیل اهمیت روزافزون حوزه‌های جنگ اطلاعاتی، کشورها معمولاً در برخورد و استفاده از فناوری‌های نوین اطلاعاتی و ارتباطی به گونه‌ای محافظه‌کارانه عمل می‌کردند و این موضوعات تا حدودی ماهیتی محرمانه داشتند. ایالات متحده هم از جمله کشورهایی بود که تا مدت‌ها پس از ظهور پدیده جنگ اطلاعات، تعریف رسمی و جامعی از جنگ اطلاعات ارائه نمی‌داد. در نهایت در اواخر دهه ۹۰، ستاد مشترک ارتش آمریکا تعریف رسمی خود از جنگ اطلاعات را ارائه نمود. این تعریف که دربرگیرنده طراحی راهبردهای نظامی این کشور در افق ۲۰۲۰ بوده است، عبارت است از: «جنگ اطلاعات دربرگیرنده اقداماتی است که طی آن تأثیرگذاری و نفوذ بر اطلاعات و سیستم‌های اطلاعاتی دشمن و همچنین دفاع از سیستم‌های اطلاعاتی و سامانه‌های ارتباطی خودی در اولویت قرار می‌گیرد». از سوی دیگر نیروی زمینی آمریکا هم تعریف خود از جنگ اطلاعات را این گونه ارائه می‌نماید: «عملیات نظامی مداوم در محیط اطلاعات نظامی که موجبات توانمند کردن، ارتقاء و حفظ چرخه تصمیم‌گیری فرماندهی را فراهم آورده و طی آن برتری اطلاعاتی در عملیات نظامی تحقق پیدا می‌کند». (Henry Fredrick, 2005: 122)



همچنین نیروی دریایی این کشور برداشت خود از جنگ اطلاعات را به این شرح ارائه می کند: «همه اقداماتی که در راستای حمایت از راهبرد امنیت ملی آمریکا با هدف کسب و حفظ برتری قطعی با حمله به سیستم‌ها و زیرساخت های اطلاعاتی دشمن از طریق بهره برداری، تاثیرگذاری و حفاظت از زیرساخت های اطلاعاتی خودی انجام می شود». و در نهایت نیروی هوایی آمریکا تعریف زیر را در ارتباط با جنگ اطلاعات مطرح می نماید: «اقداماتی که با هدف رسیدن به برتری اطلاعاتی از طریق تاثیرگذاری بر اطلاعات، سامانه‌ها و سیستم‌های اطلاعاتی و شبکه‌های مبتنی بر رایانه و همچنین دفاع از اطلاعات و سامانه‌های اطلاعاتی خودی انجام می شود».<sup>۱</sup> (Ibid: 130-133)

با توجه به آنچه مورد بررسی قرار گرفت، از نگاه ارگان ها و نهادهای نظامی ایالات متحده آنچه در این حوزه مهم می نماید، حمله به زیرساخت های اطلاعاتی و فرآیند تصمیم گیری فرماندهی دشمن و در مقابل حفاظت و حراست از زیرساخت ها و سیستم‌های اطلاعاتی خودی و به نوعی جلوگیری از دسترسی دشمن به اطلاعات نیروهای خودی، راهبرد اصلی این کشور در حوزه جنگ اطلاعات می باشد.

### روسیه

بعد از ظهور جنگ اطلاعات به عنوان یکی از حوزه‌های تحول آفرین در مسائل امنیتی جهان معاصر، روس ها زودتر از دیگران به استقبال آن شتافتند. برجسته بودن مباحث مختلف اطلاعاتی و دیدگاه‌های مبتنی بر رویکردهای اطلاعاتی و امنیتی از ابتدا در محافل نظامی روسیه وجود داشته است. در مجله معروف «تفکر نظامی»<sup>۱</sup> که دانشکده فرماندهی ستاد مشترک روسیه آن را منتشر می نماید «اس ای بوگدانف»<sup>۲</sup> می نویسد: «رسیدن به اهداف جنگ‌های معاصر را می توان با استفاده از شیوه‌های نظامی، اقتصادی و درگیری اطلاعاتی - روانی و اطلاعاتی - فنی محقق نمود».

کاپیتان بیکترین معتقد است که جنگ‌های اطلاعاتی، چندلایه است. چرا که در زمان صلح جنگ اطلاعاتی از حیثه عمل وسیع تری برخوردار بوده و ارگان های بیشتری درگیر آن هستند اما در زمان

۱ - Military Thought

۲ - S.A. Bogdanov

جنگ یک یا دو وزارتخانه مرتبط با این حوزه به همراه ارتش فعالیت می‌کنند. « آدمیرال ولادیمیر پیرموف»<sup>۱</sup> که زمانی مشاور علمی سابق رئیس جمهوری روسیه (پوتین) بوده است، جنگ اطلاعاتی را این چنین تعریف می‌کند: « جنگ اطلاعاتی نوع جدیدی از جنگ‌هاست که در آن از ابزارها و شیوه‌های نوین اطلاعاتی جهت تأثیرگذاری بر منابع اطلاعاتی دشمن و حفاظت از منابع اطلاعات خودی با هدف تحقق اهداف از پیش تعیین شده، استفاده می‌شود». (Gerald Fitz, 2003: 82-90)

با توجه به چند تعریف ارائه شده به نظر می‌رسد در میان تئوریسین‌های روسی یک اجماع کلی در مورد تعریف جنگ اطلاعاتی وجود ندارد. اما چارچوب‌های فکری حاکم بر جنگ اطلاعات از سوی تئوریسین‌های نظامی روسیه عبارت است از:

- تئوریسین‌های روسی همچون آمریکایی‌ها بر حفاظت از اطلاعات خودی و تخریب اطلاعات دشمن تأکید دارند.
- توجه به مقوله « سلاح اطلاعاتی» در میان تعاریف مذکور برجسته است.
- روسیه دید وسیع‌تری نسبت به حوزه‌های عملیات اطلاعاتی دارد، چرا که اهمیت مقوله تأثیرگذاری اطلاعات را هم در زمان صلح و هم جنگ مورد بررسی قرار می‌دهد.
- بحث سرعت عمل و زمان هم از جمله مقولاتی است که در جنگ اطلاعاتی روسیه بر آن تأکید می‌شود.
- اتخاذ یک نگاه سیستمی به جنگ اطلاعات از سوی کارشناسان نظامی روس به چشم می‌خورد.
- همچنین به خاطر اهمیت مسئله چچن در روسیه، جنگ روانی-مذهبی هم به عنوان یک حوزه مهم در جنگ‌های اطلاعاتی مطرح می‌گردد. (Ibid: 96)

### چین

همچون سایر حوزه‌هایی که چینی‌ها در آن پیشرفت‌های چشمگیری داشته‌اند، در بحث جنگ اطلاعات و فضای مجازی هم همسو با سایر حوزه‌ها رشد داشته‌اند. اگر در حوزه اقتصاد چینی

۱ - Vladimir Piromov

ها همواره به الگوبرداری از سایرین و بهره برداری از آن شهرت داشته اند در زمینه جنگ اطلاعات نیز همین رویه را به گونه ای دیگر در پیش گرفته اند. تحلیل و کنکاش عمیق راهبردهای نظامی ایالات متحده در جنگ خلیج فارس و جنگ افغانستان از سوی تحلیلگران نظامی چین در دستور کار قرار گرفته و به نوعی تلاش داشته اند راهبرد ایالات متحده را با فرهنگ بومی چین تلفیق نمایند. بنابراین تلقی آنها از جنگ اطلاعات شبیه آن چیزی است که آمریکایی ها دنبال می کنند با اندکی تفاوت.

چینی ها به طور کلی به دنبال سازگار نمودن شیوه های جنگی خود با توجه نیازهای جنگ اطلاعات هستند. آنها در بحث تکنیک های جنگ اطلاعات به دنبال ترکیب عناصر سستی (دیدگاه های مائو و سان تزو) و غربی هستند. آنچه در خصوص سیستم های جنگ اطلاعاتی و فضای مجازی این کشور قابل توجه است، این است که کارشناسان نظامی و تئوریسین های فعال در این حوزه به این موضوع معترفند که پیشرفت های آنها در این حوزه فاصله قابل توجهی با کشورهایی چون ایالات متحده و روسیه دارد. (Robert Neilson, 1997: 74) اما آنچه چینی ها سخت به دنبال آن هستند، اختصاص دادن سرمایه گذاری های کلان به منظور تحقق اهداف و نیازمندی های خود در حوزه تکنیک های جنگ اطلاعات است. فعالیت های بی وقفه چینی ها در خصوص جمع آوری داده های اطلاعاتی در مورد زیرساخت های اطلاعاتی آمریکا از این حیث قابل بررسی است.

#### ماهیت منازعات آینده

با توجه به پیشرفت دانش و تکنولوژی، دستیابی دولتها به توانمندی های تسلیحاتی پیشرفته و تغییراتی که در محیط امنیتی کشورهای و نظام بین الملل ایجاد شده است ماهیت ستیزها و منازعات هم متحول شده است. مباحث این بخش برگرفته از روندهای امنیتی ۲۰۲۵ است که در سال ۲۰۰۸ توسط موسسه NIC موسسه اطلاعات ملی آمریکا منتشر گردیده است. در زیر به مهمترین جنبه های متحول منازعات آینده اشاره خواهد شد:

#### اهمیت روزافزون اطلاعات

پیشرفت تکنولوژی اطلاعاتی باعث شکل گیری سلاح های جنگی پیشرفته با دقت بالا، بهبود توانمندی های هدف گیری و نظارت و دیده بانی، فرماندهی و کنترل بهتر و استفاده بیشتر از روبات

های اطلاعاتی خواهد شد. با توجه به نقش تاثیرگذاری که فناوری های اطلاعاتی در قابلیت های جنگی مدرن خواهند داشت. پیش بینی می شود که خود موضوع اطلاعات، هدف عمده منازعات آینده باشد. تا سال ۲۰۲۵ برخی از کشورها احتمالاً از سلاح هایی استفاده می کنند که جهت تخریب و نابودی سیستم ها و شبکه های اطلاعاتی، حس گر ها و سیستم های ارتباطی طراحی شده اند. مثلاً سلاح های ضد ماهواره، ضد رادیو فرکانس و سلاح های لیزری. (Global Trends 2025:60-65)

### تحول در توانمندی کشورها و پتانسیل های جنگی غیر متعارف

از ویژگی های مهم و اساسی منازعات در سال ۲۰۲۵ استفاده دولت ها و بازیگران غیردولتی از تاکتیک های جنگی غیر معمول به عنوان راهکار جنگی در مواجهه با نیروهای نظامی پیشرفته خواهد بود. تکنولوژی های ارتباطی پیشرفته همچون ماهواره، اینترنت، تلفن همراه، روش های جدید تجاری و سیستم های اطلاعاتی با ظرفیت بسیار بالا که حجم قابل توجهی از متون، نقشه و تصاویر دیجیتالی و فیلم را در خود جای می دهند، به شکل گسترده ای نیروهای غیر متعارف را قادر می سازد که بتوانند عملیات های مخربی را سازماندهی کرده و در این امر از هماهنگی و انسجام بیشتری برخوردار باشند. (Ibid:66)

### گسترش حوزه منازعات فراتر از عرصه های جنگ سنتی

پیش بینی می شود که امکان جلوگیری از گسترش ستیزها در آینده بسیار مشکل است. پیشرفت و گسترش قابلیت های هسته ای (مانند سلاح های با برد طولانی و دقت بالا) و تولید مداوم سلاح های کشتار جمعی و استفاده از اشکال نوین جنگی مثل جنگ مجازی یا جنگ فضایی ابزارهایی را در اختیار نظامیان دولت ها و گروه های غیر دولتی قرار می دهد که می توانند منازعات آینده را فراتر از عرصه های جنگ سنتی گسترش دهند. (Ibid: 67)

### روش تحقیق

دلفی به عنوان شیوه ای در مشاوره، روش مناسبی برای ترسیم نمایی کلی از رویدادهای جاری در حوزه علم است. این روش، اغلب دارای فرایندی دو مرحله ای است که با هدف آگاهی از دیدگاه های مقدماتی گسترده وسیعی از صاحب نظران، کار خود را با یک نظر سنجی

پیرامون موضوع آغاز می کند. سپس پاسخ ها تلفیق (مقابله و تراز یابی) شده و برای نظر خواهی دوباره از شرکت کنندگان، ارسال می گردد. هر تکرار شامل یک «دوره» بوده، و وسیله ای برای بیان دیدگاه های کارشناسان است. نتایج هر دور نظرسنجی جمع آوری شده و اظهار نظر ها به شیوه های کمی و کیفی تحلیل می شود. شمار دور های مورد نیاز بستگی به سطح اجماعی دارد که پیمایش و تحقیق به دنبال دستیابی به آن است. (خزایی و پدرام، ۱۳۸۷: ۵۸)

بر این اساس در تحقیق حاضر، ۵۰ نفر از متخصصان و کارشناسان مورد شناسایی قرار گرفته و دیدگاه های آنان در خصوص تحولات احتمالی آینده امنیتی آن حوزه مورد پرسش قرار می گیرد. در این تحقیق پس از تحلیل نظرات کارشناسان حوزه امنیتی منازعات و جنگ های اطلاعاتی، سناریو های احتمالی و به دنبال آن فرصت ها و چالش های احتمالی آینده مورد بررسی قرار می گیرد. شمار سوالات طراحی شده به گونه ای کلی و دربرگیرنده ۱۰ سوال است که پاسخ های ارائه شده تحقیق، نگارنده را در ارائه سناریو های امنیتی در باب موضوع مذکور باری رسانده است. لازم به ذکر است که لیست نهادها و مراکزی که پرسشنامه دلفی در آن جا به انجام رسیده به ضمیمه مقاله به فصلنامه ارائه شده است. شیوه انجام تحقیق و به عبارتی روش تحقیق در چارچوب محورهای زیر قابل بررسی است:

#### شیوه نمونه گیری

نمونه گیری یعنی انتخاب تعدادی از افراد، حوادث و اشیاء از یک جامعه تعریف شده به عنوان نماینده آن جامعه. جامعه مورد نظر، جامعه ای است که مورد قبول اغلب محققان قرار گرفته است. این جامعه عبارت است از همه اعضای واقعی یا فرضی که علاقمند هستیم یافته های پژوهش را به آنها تعمیم دهیم. (دلاور، ۱۳۸۲: ۱۱۰-۱۰۲) نمونه گیری دربرگیرنده روش های مختلفی است همچون: تصادفی ساده، منظم یا سیستماتیک، طبقه ای، خوشه ای، داوطلبانه و ... در این تحقیق و بر اساس روش دلفی نمی توان به صراحت یکی از روش های مذکور را مورد توجه قرار داد. به نظر می رسد با توجه به اینکه در روش دلفی انتخاب تعداد نخبگانی که درگیر در حوزه مورد نظر هستند برای تحلیل و تبیین مباحث مورد بررسی قرار می گیرند، می توان شیوه مبتنی بر شناسایی نخبگان فعال در حوزه مورد بحث درگیر در مباحث مربوط به جنگ های آینده را در نظر گرفت. شیوه نمونه گیری در این تحقیق به این صورت

بود که گروهی از متخصصان و افراد تاثیرگذار در حوزه مباحث امنیتی به ویژه جنگ‌های آینده مورد شناسایی قرار گرفتند. تعداد این افراد تحقیق حاضر و به عبارتی نمونه‌های تحقیق مشتمل بر ۵۰ نفر بوده است. بخش اعظمی از کار نمونه گیری بر این اساس صورت گرفته که با انتخاب یک نخبه در حوزه مورد بحث از وی خواسته شده تا سایر متخصصان و تصمیم گیران آن حوزه را معرفی نماید.

### ابزار گردآوری داده‌ها

یکی از شیوه‌های مرسوم گردآوری داده‌های تحقیق استفاده از پرسشنامه است. معمولاً پرسشنامه برای جمع آوری اطلاعات مورد نظر به صورت طرح سوالات دو بخشی یا انتخاب های چندگانه و چندگزینه ای مورد استفاده قرار می گیرد. (اساکول، ۱۳۸۶: ۵۲) در تحقیق مذکور در کنار بهره گیری از روش پرسشنامه از مصاحبه نیز استفاده شده است؛ به این صورت که بعد از طراحی پرسشنامه برای تبیین و تحلیل هر چه بهتر داده‌ها با هدف کمک به گردآوری داده‌های دقیق تر و صرفه جویی در وقت و همچنین بالا رفتن اهمیتی که پرسشنامه و موضوع تحقیق برای فرد پاسخ دهنده دارد، عمدتاً در کنار پرسشنامه از شیوه مصاحبه نیز استفاده گردید. سوالات پرسشنامه به صورت گزینه‌ها یا انتخاب های چندگانه و به شیوه لیکرت انجام شده است. در این تحقیق پرسشنامه لیکرت به دو صورت: ۱) خیلی زیاد، زیاد، متوسط، کم، اصلاً (خیلی کم) و ۲) کاملاً موافق، موافق، بی تفاوت، مخالف و کاملاً مخالف طراحی شده است. با هدف ارزیابی و دقت بیشتر در سوالات، پرسشنامه یک بار قبل از ارائه به پاسخ دهندگان مورد نظر، به صورت آزمایشی اجرا گردید. پیشنهادهای مختلف در راستای اصلاح پرسشنامه و رسیدن آن به سطح کیفی مطلوب، از طریق فرآیند اجرای آزمایشی پرسشنامه<sup>۱</sup> مورد توجه و ارزیابی قرار گرفت.

<sup>۱</sup> - Pre Test

تحلیل داده‌ها (یافته‌ها)

توصیف پاسخگویان

عنوان	ویژگی پاسخگویان	فراوانی	درصد فراوانی
جنسیت	زن	۸	۱۶,۰
	مرد	۴۲	۸۴,۰
سن	۲۰ - ۳۰	۱۰	۲۰,۰
	۳۰ - ۴۰	۲۵	۵۰,۰
	۴۰ - ۵۰	۹	۱۸,۰
	۵۰ - ۶۰	۶	۱۲,۰
تحصیلات	لیسانس	۵	۱۰,۰
	فوق لیسانس	۲۲	۴۴,۰
	دکتری	۲۳	۴۶,۰
شغل	اجرایی	۱۸	۳۶,۰
	استاد دانشگاه	۱۶	۳۲,۰
	محقق	۱۶	۳۲,۰

همان طور که در جدول بالا مشاهده می شود، جامعه آماری ۵۰ نفره این تحقیق متشکل از کارشناسان، متخصصان و تصمیم گیران مباحث و روندهای امنیتی در چهار مقوله جنسیت، سن، تحصیلات و شغل تقسیم بندی شده است. بر این اساس:

- از نظر جنسیت؛ ۸۴ درصد مرد و ۱۶ درصد زن بوده اند.
- از نظر ترکیب سنی؛ ۲۰ درصد از پاسخ دهندگان ۲۰ تا ۳۰ ساله، ۵۰ درصد ۳۰ تا ۴۰ ساله، ۱۸ درصد ۴۰ تا ۵۰ ساله و ۱۲ درصد ۵۰ تا ۶۰ ساله بوده اند.
- از لحاظ تحصیلات؛ ۱۰ درصد لیسانس، ۴۴ درصد فوق لیسانس و ۴۶ درصد دکترا بوده‌اند.

- از لحاظ تقسیم بندی شغلی؛ ۳۶ درصد اجرایی، ۳۲ درصد استاد دانشگاه و ۳۲ درصد نیز محقق بوده اند.

علاوه بر توصیف عددی جامعه آماری آن چه در اینجا توجه به آن ضروری است، بحث جایگاه و حیطه تاثیرگذاری کارشناسان و میزان درگیری ذهن آنها در ساختن آینده است. در این تحقیق سعی شد تا حد امکان شاخص ترین افراد در حوزه مورد بحث برای پاسخگویی انتخاب شوند. تمرکز فعالیت های پژوهشی نگارنده از آغاز مقطع دکتری بر روی مباحث آینده پژوهی و به دنبال آن مطالعه روندهای امنیتی به شناخت اینجانب از متخصصان و کارشناسان حوزه مذکور یاری رساند و از سوی دیگر برای استخراج داده‌های متقن سعی شد از نخبگان و متخصصانی که در ابتدا به صورت محدود انتخاب شدند، خواسته شود که از طرق مختلف سایر کارشناسان و دست اندرکاران اجرایی را برای پاسخگویی به پرسشنامه و انجام مصاحبه، معرفی نمایند. اگرچه بر اساس شیوه تحقیق مطالعات دلفی، یکی از ویژگی های این نوع پژوهش ها گمنامی پاسخ دهندگان است اما در ارتباط با نهادها و سازمان های مطرح در حوزه مطالعات امنیت ملی و امنیت بین الملل همان طور که در ابتدای تحقیق گفته شد، اسامی این نهادها به دفتر فصلنامه ارائه شده است. مولفه‌هایی چون، امنیت ملی، امنیت بین الملل، تحقیقات امنیتی راهبردی، منابع موثر در تصمیم گیری های کلان امنیتی، مصاحبه با افرادی که در بحث جنگ‌های اطلاعات و فضای سایبر، الکترونیک و رسانه فعال هستند و ... از جمله ساختارهای تعیین کننده نهادهای مذکور برای انجام تحقیق بوده است.

### توصیف و تحلیل گویه‌های اصلی

تا چه اندازه معتقدید که جنگ اطلاعات در آینده (تا ۲۰۲۵) بیشترین تهدید را برای امنیت ملی جمهوری اسلامی ایران در پی خواهد داشت؟

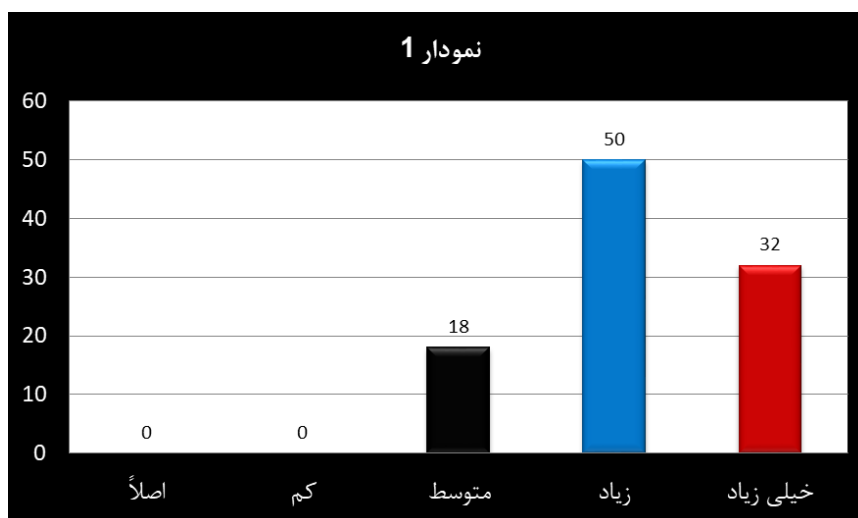
جدول شماره (۱)

جنگ اطلاعات / امنیت ملی	فراوانی	درصد فراوانی
اصلاً	0	۰.0
کم	۰	۰.0
متوسط	9	18.0



50.0	25	زیاد
32.0	16	خیلی زیاد
100.0	50	کل

بر طبق داده‌های جدول شماره ۱، نسبت پاسخگویان به ارتباط جنگ اطلاعات و تهدید امنیت ملی ج.ا.ا، ۱۸ درصد متوسط، ۵۰ درصد زیاد و ۴۲ درصد خیلی زیاد است. در مجموع ۸۲ درصد از آنان ارتباط معنادار بین دو متغیر را زیاد و خیلی زیاد دانسته اند. اجماع حاصل از این سوال نشان می دهد که جنگ اطلاعات در آینده بیشترین تهدید را برای امنیت ملی جمهوری اسلامی ایران خواهد داشت.



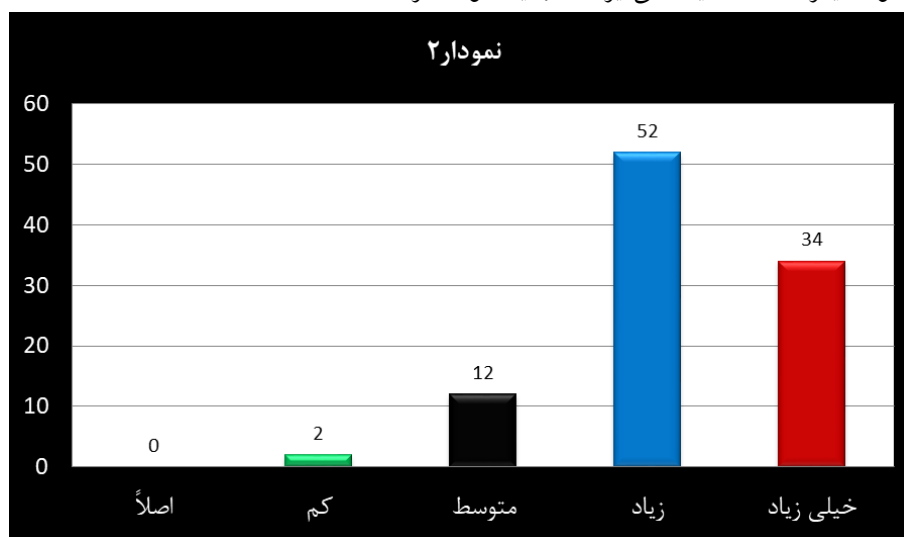
به نظر شما تا چه اندازه اقدامات قدرت های بزرگ از طریق رسانه‌ها (ماهواره، اینترنت و ...) امنیت ملی ایران را تهدید خواهد کرد.»

جدول شماره (۲)

درصد فراوانی	فراوانی	رسانه / امنیت ملی
۰.۰	0	اصلاً
2.0	1	کم
12.0	6	متوسط

52.0	26	زیاد
34.0	17	خیلی زیاد
100.0	50	کل

در جدول شماره ۲ چنان چه مشاهده می شود نسبت پاسخگویان به تاثیر اقدامات قدرت های بزرگ از طریق رسانه بر امنیت ملی ۲ درصد کم، ۱۲ درصد متوسط، ۵۲ درصد زیاد و ۳۴ درصد خیلی زیاد است. در مجموع ۸۶ درصد از پاسخگویان ارتباط معنادار دو متغیر را زیاد و خیلی زیاد دانسته اند. بر این اساس اجماع حاصل از این سوال نشان می دهد که اقدامات قدرت های بزرگ از طریق رسانه ( ماهواره، اینترنت و ...) امنیت ملی ایران را تهدید خواهد کرد.



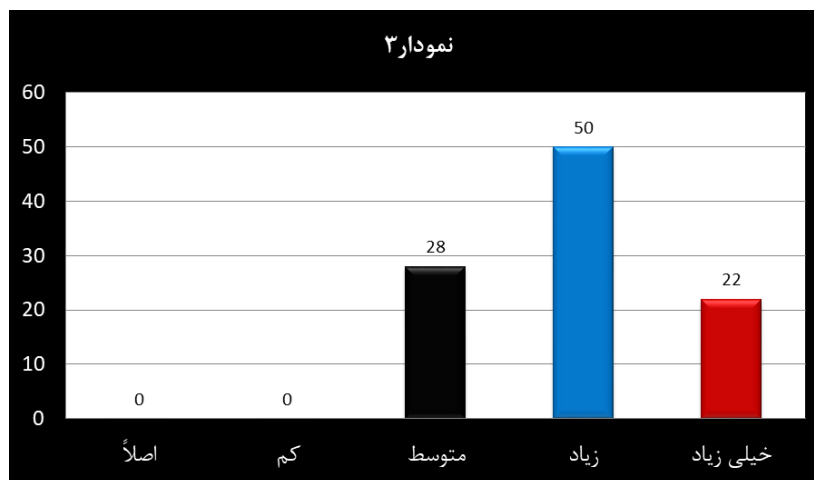
به نظر می رسد ماهواره‌ها نسبت به سایر وسایل ارتباطی نوین همچنان بیشترین تاثیر را بر فرهنگ و ارزش های اجتماعی جامعه ایران داشته باشد. گزاره فوق را تا چه حد قبول دارید؟

جدول شماره (۳)

درصد فراوانی	فراوانی	ماهواره/ ارزش های فرهنگی
۰.۰	0	اصلاً
۰.۰	۰	کم

متوسط	14	28.0
زیاد	25	50.0
خیلی زیاد	11	22.0
کل	50	100.0

چنان چه مشاهده می شود در جدول شماره ۴ نسبت تاثیر پاسخگویان به تاثیر ماهوارهها بر فرهنگ و ارزش های اجتماعی جامعه ایران، ۲۸ درصد متوسط، ۵۰ درصد زیاد و ۲۲ درصد خیلی زیاد است. در مجموع ۷۲ درصد از آنان ارتباط معنادار بین دو متغیر را زیاد و خیلی زیاد دانسته اند. اجماع حاصل نشان می دهد که ۷۲ درصد از پاسخگویان تاثیر ماهوارهها بر فرهنگ و ارزش های اجتماعی جامعه ایران در آینده را زیاد و خیلی زیاد دانسته اند.



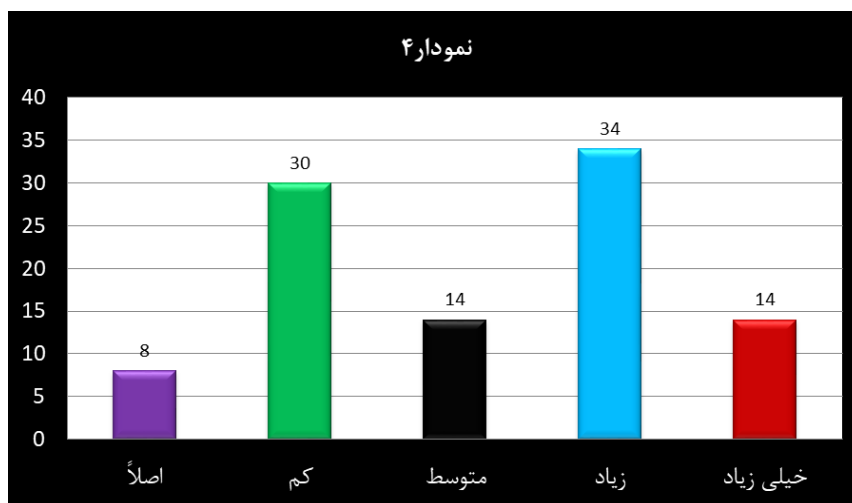
بررسی روندهای مختلف معطوف به آینده نشان می دهد که « تجاوز به حریم خصوصی» جدی ترین نگرانی کشورها در حوزه های جنگ اطلاعاتی آینده باشد. تا چه حد موافق این جمله هستید؟

جدول شماره (۴)

تجاوز به حریم خصوصی	فراوانی	درصد فراوانی
---------------------	---------	--------------

۸,۰	۴	اصلاً
30.0	15	کم
۱۴,۰	۷	متوسط
۳۴,۰	۱۷	زیاد
۱۴,۰	۷	خیلی زیاد
100.0	50	کل

بر اساس داده جدول شماره ۶، نسبت پاسخگویان به ارتباط مولفه تجاوز به حریم خصوصی با جدی‌ترین نگرانی آینده کشورها، ۸ درصد اصلاً (خیلی کم)، ۳۰ درصد کم، ۱۴ درصد متوسط، ۳۴ درصد زیاد و ۱۴ درصد خیلی زیاد است. سوال فوق از جمله سوال‌هایی است که در این پروژه بر سر آن اجماعی به دست نیامد ناگزیر یک بار دیگر پرسشنامه به تغییراتی جزئی همراه با پاسخنامه سایر افراد در اختیار فرد پاسخ دهنده قرار گرفت که نتایج مذکور به دست آمد که باز هم اجماع حاصل نگردید. بنابراین داده‌های پژوهش در این سوال در دو دسته سناریو قابل تحقق است: ۴۷ درصد از پاسخ دهندگان تجاوز به حریم خصوصی را به مقدار زیاد و خیلی زیاد جدی‌ترین نگرانی کشورها در آینده می‌دانند و ۳۸ درصد نیز این نگرانی را کم و اصلاً (خیلی کم) دانسته‌اند.

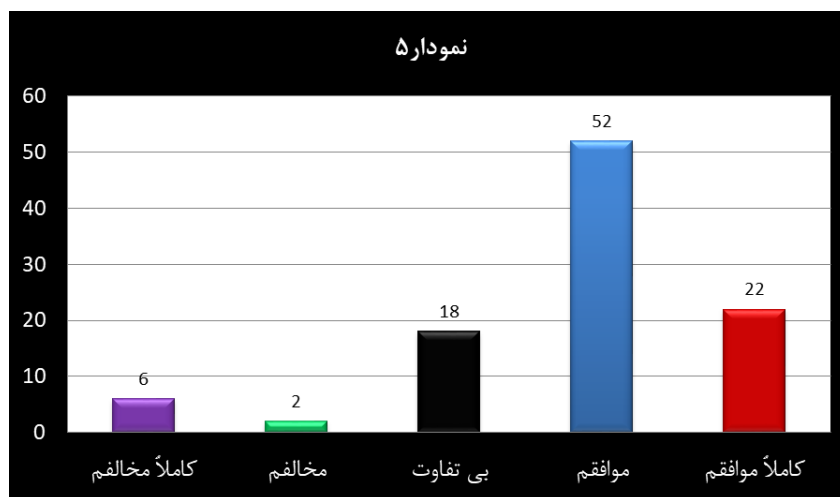


چقدر با این جمله موافقت می کنید که توانمندی جمهوری اسلامی در فضای متحول جنگ های آینده (فضای مجازی) به مراتب فراتر از جنگ های سنتی و سخت خواهد بود؟

جدول شماره (۵)

درصد فراوانی	فراوانی	تجارت الکترونیک/ منافع ملی
6.0	3	کاملاً مخالفم
2.0	1	مخالفم
18.0	9	بی تفاوت
52.0	26	موافقم
22.0	11	کاملاً موافقم
100.0	50	کل

بر طبق داده های جدول شماره ۷ در مورد اهمیت تجارت الکترونیک برای منافع ملی ج.ا.ا در آینده، ۶ درصد از پاسخ دهندگان کاملاً مخالف، ۲ درصد مخالف، ۱۸ درصد بی تفاوت، ۵۲ درصد موافق و ۲۲ درصد کاملاً موافقت کردند. اجماع نظرات نشان می دهد که ۷۴ درصد از پاسخ دهندگان در مورد اینکه تجارت الکترونیک در آینده برای منافع ملی ج.ا.ا مفید خواهد بود، موافق و کاملاً موافقت کردند.

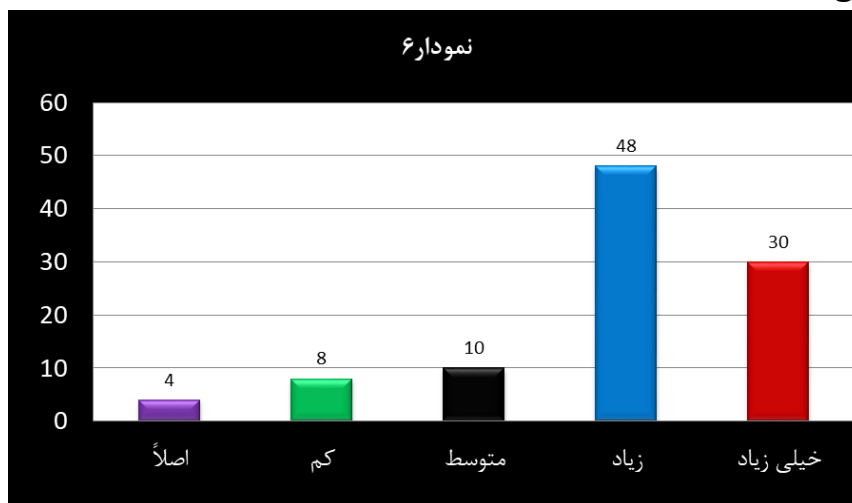


به نظر شما تا چه اندازه فناوری های جدید اطلاعات می تواند باعث ارتقاء سطح امنیت ملی جمهوری اسلامی ایران در آینده گردد؟

جدول شماره (۶)

درصد فراوانی	فراوانی	فناوری اطلاعات / امنیت ملی
4.0	2	اصلاً
8.0	4	کم
10.0	5	بی تفاوت
48.0	24	زیاد
30.0	15	خیلی زیاد
100.0	50	کل

بر طبق داده‌های پژوهش در جدول شماره ۸ نسبت پاسخگویان به ارتباط فناوری های جدید اطلاعات و ارتقاء سطح امنیت ملی ج.ا.ا در آینده، ۴ درصد اصلاً (خیلی کم)، ۸ درصد کم، ۱۰ درصد متوسط، ۴۸ درصد زیاد و ۳۰ درصد خیلی زیاد است. در مجموع ۷۸ درصد از آنان ارتقاء سطح امنیت ملی ج.ا.ا از طریق فناوری های جدید در آینده را زیاد و خیلی زیاد می دانند.

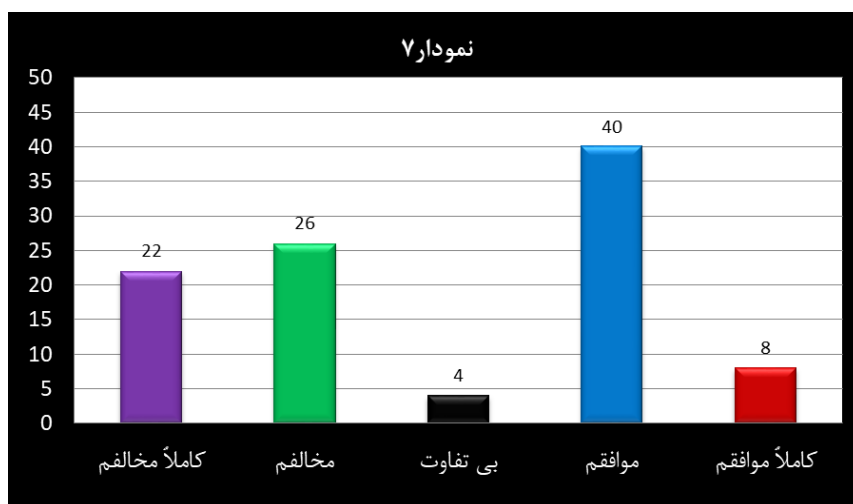


آیا با این جمله موافقید که توانایی ایران در جنگ الکترونیک، احتمال جنگ سخت میان ایران و دشمنانش را در آینده کاهش می دهد؟

جدول شماره (۷)

ایران / جنگ الکترونیک	فراوانی	درصد فراوانی
کاملاً مخالفم	۱۱	۲۲,۰
مخالفم	۱۳	۲۶,۰
بی تفاوت	۲	۴,۰
موافقم	۲۰	۴۰,۰
کاملاً موافقم	۴	۸,۰
کل	۵۰	۱۰۰.۰

بر اساس داده‌های جدول شماره ۹، نسبت پاسخ دهندگان به رابطه توان ایران در جنگ الکترونیک و کاهش احتمالی جنگ سخت ایران و دشمنانش ۲۲ درصد کاملاً مخالف، ۲۶ درصد مخالف، ۴ درصد بی تفاوت، ۴۰ درصد موافق و ۸ درصد کاملاً موافق است. سوال مذکور نیز از جمله سوال هایی بود که در مورد آن پاسخ ها از اجماع برخوردار نبود. درصدهای فراوانی مذکور نتیجه ارائه دوباره پرسشنامه به پاسخ دهندگان برای رسیدن به اجماع (بر اساس روش دلفی) است که در نهایت دو طیف از جواب ها در دو سناریو به دست آمد: ۴۸ درصد از پاسخ دهندگان با این عبارت که توانایی ایران در جنگ الکترونیک احتمال جنگ سخت میان ایران و دشمنانش در آینده را کاهش می دهد موافق و کاملاً موافقت و ۴۸ درصد نیز با این گزاره مخالف و کاملاً مخالفند.



تا چه اندازه با این جمله موافقت می‌کنید که تقابل ایالات متحده با جمهوری اسلامی ایران در حوزه جنگ‌های اطلاعاتی در آینده در ابعاد جدیدی ادامه خواهد یافت؟

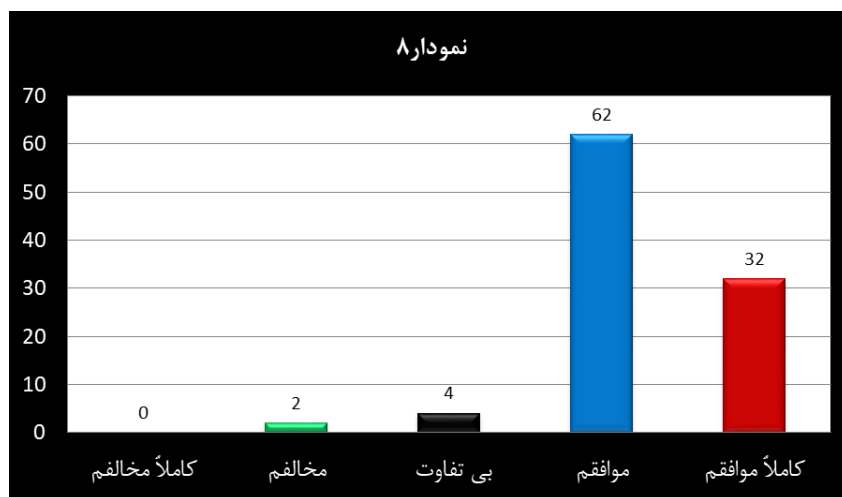
جدول شماره (۸)

درصد فراوانی	فراوانی	جنگ اطلاعاتی ایران و آمریکا
۰.۰	۰	کاملاً مخالفم
۲.۰	۱	مخالفم
۴.۰	۲	بی تفاوت
۶۲.۰	۳۱	موافقم
۳۲.۰	۱۶	کاملاً موافقم
۱۰۰.۰	۵۰	کل

چنانچه مشاهده می‌شود در جدول شماره ۱۲، درصد جواب پاسخ دهنده‌ها در مورد تقابل ایالات متحده با جمهوری اسلامی ایران در حوزه جنگ‌های اطلاعاتی در ابعاد جدید در آینده، ۲ درصد مخالف، ۴ درصد بی تفاوت، ۶۲ درصد موافق و ۳۲ درصد کاملاً موافق است. اجماع به دست آمده در این سوال نشان می‌دهد که ۹۴ درصد از پاسخ دهنده‌ها در مورد اینکه



تقابل ایالات متحده با جمهوری اسلامی ایران در حوزه جنگ های اطلاعاتی در آینده ادامه خواهد داشت موافق و کاملاً موافقمند.

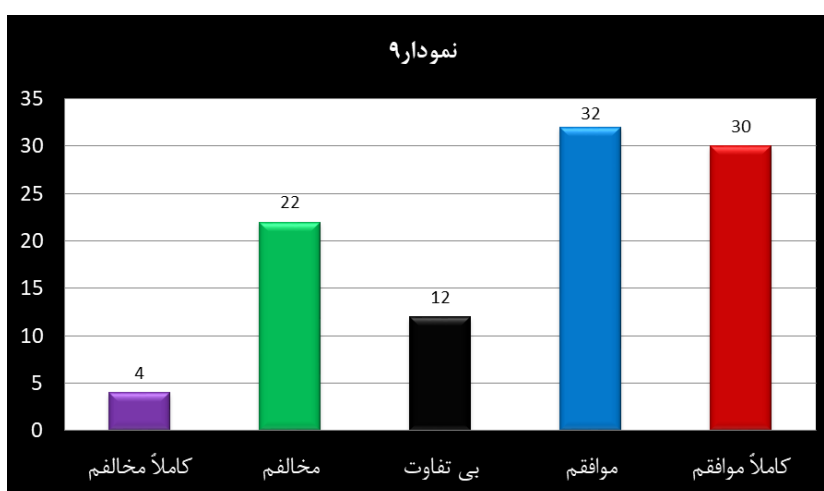


تا چه حد با این جمله موافقت می کنید که حمله به زیرساخت های حیاتی کشور مثل تأسیسات سوخت رسانی، نیروگاه های برق، ارتباطات و حمل و نقل یکی از مهمترین ابزارهای جنگ سایبری غرب علیه ایران باشد.

جدول شماره (۹)

درصد فراوانی	فراوانی	حوزه های نفوذ قدرت های بزرگ / جنگ های آینده
4.0	2	کاملاً مخالفم
22.0	11	مخالفم
12.0	6	بی تفاوت
32.0	16	موافقم
30.0	15	کاملاً موافقم
100.0	50	کل

داده‌های به دست آمده در جدول شماره ۱۹ بیانگر آن است که نسبت پاسخگویان در مورد احتمال حمله به زیرساخت های حیاتی کشور مثل تاسیسات سوخت رسانی، نیروگاه های برق و... ۴ درصد کاملاً مخالف، ۲۲ درصد مخالف، ۱۲ درصد بی تفاوت، ۳۲ درصد موافق و ۳۰ درصد کاملاً موافق است. اجماع حاصل نشان می دهد که ۶۲ درصد از پاسخگویان با این عبارت موافق و کاملاً موافقتند که حمله به زیرساخت های حیاتی کشور مثل تاسیسات سوخت رسانی، نیروگاه های برق، ارتباطات و حمل و نقل یکی از مهمترین ابزارهای جنگ سایبری غرب علیه ایران خواهد بود.



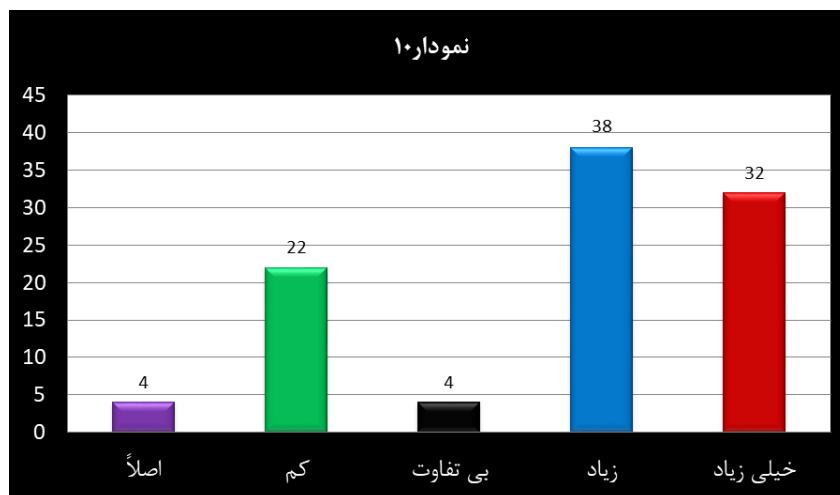
تا چه حد موافق این جمله هستید که اگرچه جنگ اطلاعات در آینده نقش محوری خواهد داشت اما کماکان قدرت نظامی کلاسیک، تعیین کننده جایگاه قدرت ها در عرصه نظام بین الملل است؟

جدول شماره (۱۰)

درصد فراوانی	فراوانی	قدرت نظامی کلاسیک / جایگاه قدرت ها
4.0	2	خیلی کم
۲۲,۰	۱۱	کم
4.0	۲	متوسط
۳۸,۰	۱۹	زیاد

32.0	۱۶	خیلی زیاد
100.0	50	کل

بر اساس داده‌های پژوهش در جدول شماره ۲۴، نسبت پاسخ دهندگان در مورد قدرت نظامی کلاسیک و جایگاه قدرت ها در نظام بین‌الملل ۴ درصد اصلاً (خیلی کم)، ۲۲ درصد کم، ۴ درصد متوسط، ۳۸ درصد زیاد و ۳۲ درصد خیلی زیاد است. در مجموع اجماع حاصل نشان می دهد که ۷۰ درصد از پاسخ دهندگان این احتمال را که جنگ اطلاعات در آینده نقش محوری خواهد داشت اما کماکان قدرت نظامی کلاسیک تعیین کننده جایگاه قدرت ها در عرصه نظام بین‌الملل خواهد بود را زیاد و خیلی زیاد می دانند.



در اینجا به طور کلی باید اذعان نمود که در موارد زیر اجماع نسبی بین پاسخ دهندگان حاصل گردید:

- (۱) جنگ اطلاعات در آینده (تا ۲۰۲۵) بیشترین تهدید را برای امنیت ملی جمهوری اسلامی ایران در پی خواهد داشت.
- (۲) اقدامات قدرت های بزرگ از طریق رسانه ( اینترنت، ماهواره و ...) امنیت ملی جمهوری اسلامی را همچنان تهدید خواهد کرد.
- (۳) تاثیر ماهواره‌ها بر فرهنگ و ارزش‌های اجتماعی جامعه ایران در آینده زیاد و بسیار زیاد خواهد بود.

- ۴) محتمل است که مقوله «تجاوز به حریم خصوصی» یکی از جدلی‌ترین نگرانی‌های کشورهای در حوزه‌های جنگ اطلاعاتی آینده باشد.
- ۵) توانمندی جمهوری اسلامی در فضای متحول جنگ‌های آینده (فضای مجازی) به مراتب فراتر از جنگ‌های سنتی و سخت خواهد بود.
- ۶) فناوری‌های جدید اطلاعات می‌تواند تا حد زیادی باعث ارتقاء سطح امنیت ملی جمهوری اسلامی ایران گردد.
- ۷) توانایی ایران در جنگ الکترونیک اصولاً به این معنی نیست که احتمال جنگ سخت میان ایران و دشمنانش در آینده کاهش می‌یابد.
- ۸) تقابل ایالات متحده با جمهوری اسلامی ایران در آینده در حوزه جنگ‌های اطلاعاتی در ابعاد جدیدی ادامه خواهد یافت.
- ۹) حمله به زیرساخت‌های حیاتی کشور مثل تأسیسات سوخت رسانی، نیروگاه‌های برق، ارتباطات و حمل و نقل یکی از ابزارهای جنگ سایبری غرب علیه ایران در جنگ‌های آینده خواهد بود.
- ۱۰) اگرچه جنگ اطلاعات در آینده نقش محوری را خواهد داشت اما کماکان قدرت نظامی کلاسیک تعیین‌کننده جایگاه قدرت‌ها در عرصه نظام بین‌الملل خواهد بود.

#### نتیجه‌گیری و سناریوهای تحقیق (در قالب فرصت‌ها و چالش‌ها)

شناسایی چالش‌های استراتژیک و تهدیدات احتمالی و اتخاذ راهکارهای مناسب برای مقابله با آن و همچنین شناسایی ظرفیت‌ها و پتانسیل‌هایی که به صورت بالقوه و بالفعل دربرگیرنده فرصت برای جمهوری اسلامی ایران می‌باشد، هدف نگارش تحقیق حاضر بوده است. ورود ناگزیر کشورها به عصر ارتباطات و فناوری اطلاعات بیانگر تصدیق چندلایه شدن امنیت بر اساس چارچوب نظری پیروان مکتب کپنهاک است. اگرچه در اینجا به نقش و اهمیت جنگ‌های کلاسیک در آینده همچنان صحنه گذاشته می‌شود اما تحولات نوین حاکی از این است که پیشرفت‌های چشمگیر در فناوری

اطلاعات و ارتباطات نقش هدایت کننده، تنظیم و کنترل جنگ‌ها را بر عهده می‌گیرد. به گونه‌ای می‌توان گفت از اهمیت جنگ‌های کلاسیک کاسته نمی‌شود بلکه ظهور شیوه‌های جدیدی از جنگ‌ها تحت عنوان جنگ اطلاعات فراتر از جنگ‌های کلاسیک تعیین کننده خواهد بود.

به تحلیل داده‌ها و یافته‌های تحقیق اختصاص داشته است. ترسیم فضای اجرای کار به طور کلی که دربرگیرنده شیوه نمونه‌گیری، ابزار گردآوری داده‌ها و در نهایت تحلیل و توصیف گویه‌های اصلی تحقیق در قالب جدول و نمودار است، در این فصل مورد اشاره قرار می‌گیرد. بخش عمده‌ای از سوال‌های پرسشنامه که در مورد آنها در مرحله اول اجرا، اجماع نسبی حاصل گردید در گفتار نهایی این فصل تحت عنوان تحلیل داده‌ها و یافته‌های تحقیق عنوان شده است.

در مجموع و بر اساس داده‌های جمع‌آوری شده در مورد اهمیت هر کدام از ابعاد جنگ‌های اطلاعات در آینده سه نگاه مختلف وجود داشت. (۱) گروهی که معتقد به اهمیت بیشتر جنگ سایبری و الکترونیک در فضای جنگ‌های متحول آینده هستند، بر این باورند که چون بهره‌گیری از ابزارهای سایبرنتیک خود مقدمه اصلی ایجاد جنگ‌های رسانه‌ای و به تبع آن جنگ روانی محسوب می‌شود و همچنین به این خاطر که فعلاً مبنای این تکنولوژی‌ها بومی نیست و فضای شکل‌گیری آنها عمدتاً در غرب است، لذا تا زمانی که جمهوری اسلامی ایران بتواند اشراف همه‌جانبه‌ای بر تکنولوژی‌های فعال در فضای سایبر داشته باشد و با توجه به تجربه بیشتر غرب در استفاده از این ابزارها، این حوزه‌ها در آینده از اهمیت بیشتری برخوردار خواهد بود. توجیه دیگر این گروه از پاسخ‌دهندگان این است که چون جنگ‌های الکترونیک و سایبری به عنوان ابزار جدیدی علیه جمهوری اسلامی به کار گرفته شده‌اند، پاسخ مشخصی از خود ارائه نکرده‌اند. به عبارت دیگر جنگ‌های روانی به دلیل رسوخی که در راهکارهای مقابله با ایران در دهه‌های گذشته داشته‌اند منجر به آمادگی بیشتر جمهوری اسلامی ایران شده و لذا خطرات کمتری را متوجه کشور می‌سازد. (۲) عده‌ای هم که معتقد به اهمیت جنگ رسانه‌ای در آینده هستند، بر این باورند که با توجه به اینکه مهمترین نقطه قوت جمهوری اسلامی بر خورداری از ارزش‌های دینی و فرهنگی و همچنین اعتماد عمومی است، دشمنان همه تلاش خود را در مسیر تضعیف این مقوله‌ها و در نتیجه تضعیف نظام به کار خواهند بست، البته در دل این پاسخ هم اهمیت فضای سایبر برجسته است اما متغیر

اصلی اعتماد عمومی و به نوعی ارزش‌های فرهنگی جامعه ایران است. ۳) گروه سومی هم در میان پاسخ دهندگان وجود دارند که تاکید بر شکل خاصی از جنگ‌های اطلاعات در آینده را مطرح نمی‌کنند. این افراد بر این باورند که چون ابعاد مختلف ماهیت جنگ‌های آینده حالت علت و معلولی دارد بنابراین در هر اقدامی در عرصه جنگ اطلاعات شاهد نقش آفرینی همه ابعاد جنگ‌های اطلاعاتی خواهیم بود اما شدت و ضعف آن تفاوت خواهد داشت. به نظر این گروه تفکیک میزان تاثیرپذیری هر کدام از ابعاد جنگ‌های آینده کار مشکلی است و همه این ابعاد به نوعی علت و معلول یکدیگرند.

هر چند آسیب‌پذیری امنیتی دولت‌ها از فضای جنگ‌های اطلاعاتی مختص و منحصر به جمهوری اسلامی ایران نیست بلکه هر نوع حاکمیتی را مورد تهدید قرار می‌دهد، چرا که مرزهای مرسوم عینی را درنوردیده و جهانی بیرونی را به جامعه و داخل و بالعکس با تارهای مجازی متصل و مرتبط نموده است. نکته دیگر این است که نمی‌توان فضای اطلاعاتی آینده را ذاتاً تهدیدزا تلقی کرد. دستیابی به علم و تکنولوژی ساخت تجهیزات مدرن برای تاثیرگذاری و مقابله در این فضا قاعدتاً چالش‌های فرارو را به فرصت تبدیل خواهد کرد. اما جمهوری اسلامی ایران در فضای متحول جنگ‌های آینده فرصت‌های چشمگیری هم خواهد داشت که با در نظر گرفتن سیر تکاملی پیشرفت در زمینه‌های مختلف فناوری اطلاعات و ارتباطات، پیش‌بینی تحقق فرصت‌های جدید در این فضا و همچنین پتانسیل بالای علوم انسانی و فنی در تبدیل چالش‌های احتمالی به فرصت بسیار محتمل است. آن‌چه در اینجا در قالب فرصت‌ها و چالش‌های احتمالی مطرح می‌گردد نگاه کارشناسان و متخصصان حوزه‌های امنیتی در ارتباط با ماهیت جنگ‌های آینده است:

### فرصت‌ها و چالش‌های احتمالی ناشی از ماهیت متحول جنگ‌های آینده

#### فرصت‌ها

- با توجه به ماهیت متحول منازعات آینده در ساحت نظری و عملی، تحول در منازعات آینده می‌تواند ضریب تاثیرگذاری کشورهای مختلف جهان (حتی کشورهای ذره‌های) را به واسطه تبادل اطلاعاتی افزایش دهد. از سوی دیگر قدرت‌های بزرگ نیز خیلی راحت‌تر از عرصه سخت‌افزاری جنگ‌های آسیب‌پذیر می‌شوند. نتیجه طبیعی این روند می‌تواند برای جمهوری اسلامی

ایران که با توجه به روندهای کنونی محتمل است یکی از محورهای این منازعات باشد، بسیار اهمیت داشته و فرصت زا باشد.

- یکی دیگر از سویه‌های احتمالی جنگ‌های آینده، توجه به مولفه «هزینه و سرمایه» است. جنگ افزارهای سخت بسیار هزینه بر بوده و نیازمند صرف هزینه‌های هنگفتی است. با توجه به حرکت جنگ از سویه سخت افزاری به نرم افزاری هزینه‌های توانایی دفاعی کشورها به ویژه کشورهایی که به مانند قدرت های بزرگ، توان صرف هزینه‌های کلان ندارند، کاهش می یابد. در این میان جمهوری اسلامی ایران می تواند با توجه به دو مولفه برخورداری از علم و تکنولوژی و نیروی انسانی مستعد در زمینه‌های مختلف و همچنین ایمان و اراده قوی ملت خود، بسیاری از چالش‌های موجود در حوزه جنگ‌های سایبری و شبکه ای را به فرصت تبدیل کند. در این زمینه امکان مقابله به مثل جمهوری اسلامی با توجه به برخورداری از توان نفوذ در سیستم‌های اطلاعاتی و امنیتی کشورهای معارض با نظام بسیار ساده تر از واکنش در عرصه‌های سخت افزاری است.
- با توجه به اینکه مشخصه اصلی جنگ‌های اطلاعات آینده برتری در فاکتور علم و تکنولوژی است، این امر با توجه به وجود مراکز دانشگاهی و پژوهشی فعال در زمینه ارتباطات و فناوری اطلاعات در کشور می تواند استفاده از ظرفیت های گسترده و بالای متخصصان داخلی برای مقابله با تهدیدات سایبر، الکترونیک و ... کشورهای رقیب را موجب شود. همچنین ظرفیت های بالای پدافند غیرعامل در کشور با توجه به ساختارهای موجود در کشور برای مقابله با تهدیدات غیرنظامی کشورهای متخاصم، مورد استفاده قرار می گیرد. به طور کلی، با توجه به اینکه علم و تکنولوژی ملاک برتری کشورها در جنگ‌های آینده است، برای حوزه‌های مختلف امنیتی جمهوری اسلامی ایران ایجاد فرصت خواهد کرد.
- ایجاد فضا برای تفکر استراتژیک، بررسی و شناخت دقیق محیط ملی و بین‌المللی از دیگر فرصت های جمهوری اسلامی ایران در عرصه جنگ‌های متحول آینده است. عمدتاً مشاهده روندهای امنیتی موجود در جهان مثل ۲۰۲۰، ۲۰۲۵ و ... باعث خواهد شد که در نظر گرفتن هر کدام از سناریوها تنها در حد یک احتمال ما را به تفکر در باب آینده وادارد. در اینجا فرصت مغتنم برای

شناسایی چالش‌های استراتژیک و تهدیدات احتمالی و اتخاذ راهکارهای مناسب برای مقابله با آن فراهم می‌گردد. به طور کلی حاکم شدن فضای تفکر استراتژیک بر مناسبات امنیتی به ویژه در فضای جنگ اطلاعات باعث شناخت دورنمای چالش‌ها و فرصت‌های آینده نظام خواهد شد که این موضوع فی‌الغافه برای جمهوری اسلامی یک فرصت تلقی می‌گردد.

- یکی از حوزه‌های فرصت‌زا برای جمهوری اسلامی ایران در حوزه جنگ‌های اطلاعاتی که بیشتر از اینکه نام منازعه یا جنگ را بتوان بر آن گذاشت می‌توان آن را از نتایج انقلاب اطلاعات دانست، بحث تجارت الکترونیک است. این حوزه در کشور ما هنوز فراگیر و نهادینه نشده است اما در مجموع و با توجه به محدودیت‌هایی که ممکن است در حوزه‌های غیرنفتی هم برای جمهوری اسلامی ایجاد گردد، این حوزه می‌تواند فرصت‌زا باشد.

- به نظر می‌رسد استفاده از پارازیت راهکار تاثیرگذاری برای مقابله موثر با شبکه‌های مخرب ماهواره ای نباشد، در فضای آینده جنگ‌های رسانه‌ای به نظر می‌رسد «رقابت» جای «تقابل» را بگیرد. افزایش شبکه‌های ماهواره ای رسانه ملی از جمله دلیل تشدید حوزه‌های رقابتی است. رسانه ملی بنا به نیاز با نگاه تخصصی گرایانه خود اقدام به گسترش شبکه‌های مختلف ماهواره ای و تلویزیونی خواهد کرد. اینکه ضرورت ایجاد چنین شبکه‌هایی در داخل با توجه به رقابت با شبکه‌های خارجی در دستور کار رسانه ملی قرار گیرد می‌تواند به عنوان یک فرصت تلقی گردد از این لحاظ که ممکن است حوزه‌های بیشتری از نیاز مخاطبان داخلی در رسانه ملی مورد توجه قرار گیرد.

- یکی دیگر از سناریوهای مورد نظر در مورد جنگ‌های آینده، پایین بودن حجم تلفات و خسارات است. در این گونه جنگ‌ها، مردم، محیط زیست و ... خسارت نمی‌بینند و بر خلاف جنگ‌های سنتی و کلاسیک، خسارت‌های به حداقل می‌رسد. این موضوع برای جمهوری اسلامی ایران می‌تواند به عنوان یک فرصت تلقی گردد. کشوری که در حال پیمودن مسیرهای توسعه و پیشرفت است، قاعدتاً در جنگ اطلاعات آینده کمتر دچار تلفات و خسارت می‌گردد. (در عرصه جنگ سنتی، تبعات جنگ تحمیلی ۸ ساله هنوز هم در قالب انفجار مین‌ها به جمهوری اسلامی ایران آسیب می‌رساند)



## چالش ها

- یکی از پیامدهای ورود جنگ های آینده به مقوله جنگ های اطلاعاتی کاهش موقعیت ژئوپلیتیک کشورهاست، اهمیت حوزه های عینی و سستی (موقعیت جغرافیایی، وسعت، جمعیت و ...) اگرچه همچنان به قوت خود باقی خواهد ماند اما ورود همه جانبه به فضای محتمل جنگ های اطلاعاتی به نظر می رسد به تضعیف این حوزه نسبت به گذشته بینجامد. این موضوع برای جمهوری اسلامی ایران به عنوان کشوری قدرتمند در سطح منطقه با برجسته بودن ابزارهای سستی و عینی قدرت ممکن است چالش زا باشد.
- گسترش روندهای ایجاد شبکه جمع آوری اطلاعات جاسوسی همراه با اقدام ایذایی و هکری یکی دیگر از سناریوهای محتمل آینده تا سال ۲۰۲۵ است. با توجه به احتمال به نتیجه نرسیدن تحریم ها علیه جمهوری اسلامی ایران و نگرانی از توسل به جنگ با توجه به پیامدهای مبهم آن به نظر می رسد محتمل ترین گزینه در این خصوص با هدف ایجاد اختلال در برنامه هسته ای جمهوری اسلامی ایران و ..... فضای مذکور با ویژگی حمله های سایبری به تاسیسات هسته ای کشورمان باشد. ( ابزاری که در نیروگاه بوشهر تحت عنوان ویروس استاکس نت مورد استفاده قرار گرفت)
- با توجه به پیوند میان سیاست و دیانت در جمهوری اسلامی و از آن جا که مبنای تفسیر، تحلیل و تصمیم نظام در نسبت با جهان خود و جهان بیرون، نگاه اسلامی و ایدئولوژیک است، از این رو اگر با تساهل ماهیت جنگ های آینده را « جنگ نرم» بدانیم، مهمترین چالش این نوع جنگ برای جمهوری اسلامی ایران، تلاش در جهت بی اعتبارسازی مبانی اندیشه ای و اخلاقی نظام و نخبگان است. نتیجه، مورد چالش واقع شدن نظم سیاسی اسلام گرا در حوزه داخلی و مشروعیت زدایی از نظم سیاسی و نخبگان است و هدف تغییر « تغییر از درون» را دنبال می کند و در حوزه بیرونی و بین المللی، نگاه تجدیدنظرطلبانه نظام به معنی نگاه غیرمرسوم، نظم ستیز و تهدیدآفرین تعبیر و جلوه گری می نماید.

- سناریوی دیگر در حوزه سایبر، موضوع شبکه‌های اجتماعی مجازی است. شکل‌گیری این شبکه‌ها از طریق سایت‌های خبری، وبلاگ‌های خبری و تحلیلی، گروه‌های اینترنتی، فضاها گفت و گو (چت روم‌ها)، فیس بوک، توئیتر و ... تلاش خواهند کرد در فضای ماهیت متحول جنگ‌ها به نارضایتی‌ها و ساماندهی فرآیندهای اعتراضی دامن بزنند. با توجه به برجسته بودن این فعالیت‌ها در برخی از کشورهای انقلابی منطقه در جریان تحولات اخیر، تشدید چنین فعالیت‌هایی با ابعاد و شیوه‌های جدید همواره در دستور کار خواهد بود.
- پیش‌بینی‌های این تحقیق حاکی از این است که تقابل ایالات متحده با جمهوری اسلامی ایران در حوزه جنگ‌های اطلاعاتی در آینده در ابعاد جدیدی ادامه خواهد داشت. این موضوع بسته به نحوه مواجهه و همچنین چشم‌انداز پیشرفت کشورمان در حوزه جنگ‌های اطلاعاتی هم دربرگیرنده چالش و هم فرصت است. اما با توجه به نوپا بودن ورود کشورمان به این عرصه و تجارب بالای کشورهای متخصص در بکارگیری شیوه‌های متفاوت این نوع جنگ‌ها، می‌توان گفت در کوتاه مدت برای جمهوری اسلامی ایجاد چالش خواهد کرد.
- گسترش شبکه‌های ماهواره‌ای فارسی‌زبان و فراهم شدن امکان دسترسی ساده‌تر به چنین شبکه‌های ماهواره‌ای و همچنین سایر شبکه‌ها نگرانی را در خصوص تأثیرگذاری این گونه شبکه‌ها در آینده افزایش می‌دهد. بر اساس پیش‌بینی‌ها، گسترش کمی و کیفی شبکه‌های ماهواره‌ای بدون نیاز به رسیور و دسترسی آسانتر به این شبکه‌ها حتی از طریق گوشی موبایل و سایر وسایل الکترونیک می‌تواند فضای مطلوبی را برای جریان‌سازی رسانه‌های بیگانه ایجاد نماید که این موضوع می‌تواند هنجارها و ارزش‌های فرهنگی جامعه ایران را بیش از پیش در معرض تهدیدات نرم قرار دهد.
- یکی از ابزارهایی که مخالفین نظام جمهوری اسلامی ایران در فضای جنگ‌های آینده همچنان مثل گذشته بر آن تمرکز خواهند داشت، تأثیرگذاری بیشتر بر گروه‌ها و قومیت‌های مختلف در ایران بنا به شرایط ویژه کشور در این زمینه است. القای بی‌توجهی نظام به مسائل و مشکلات آنان، ترسیم نگاه امنیتی به مسائل قومیت‌ها، ارائه تصویری مطلوب و رویایی از وضعیت زندگی

و سطح رفاه این قومیت ها که در کشورهای دیگر سکنی گزیده اند و ... از جمله اقدامات چالشی برای امنیت داخلی و به تبع آن امنیت ملی جمهوری اسلامی ایران خواهد بود که اگرچه هم اکنون نیز این اقدام صورت می گیرد اما به نظر می رسد از نظر غرب همچنان چنین راهکاری به عنوان یک راهکار تاثیرگذار در فرآیند جنگ های آینده در دستور کار خواهد بود.

## منابع

## فارسی

- ۱- اساکول، پی. (۱۳۸۴). روش‌های مطالعات آینده پژوهی، ترجمه سعید خزایی، مرکز آینده پژوهی علوم و صنایع دفاعی، معاونت اطلاع‌رسانی و خدمات علمی.
- ۲- اسلاتر، ریچارد و همکاران. (۱۳۸۶). نواندیشی برای هزاره نوبین؛ مفاهیم، روش‌ها و ایده‌های آینده پژوهی، مترجمین، عقیل ملکی فر، سید احمد ابراهیمی، وحید وحیدی مطلق، تهران؛ مرکز آینده پژوهی علوم و فناوری دفاعی، موسسه آموزشی و تحقیقاتی صنایع دفاعی.
- ۳- بوزان، باری، و ویور. (۱۳۸۰). چارچوبی تازه برای تحلیل امنیت، ترجمه علیرضا طیب، تهران؛ انتشارات پژوهشکده مطالعات راهبردی.
- ۴- دلاور، علی (۱۳۸۲). روش‌های تحقیق در روانشناسی و علوم تربیتی، تهران؛ انتشارات دانشگاه پیام نور.
- ۵- روزنا، جیمز و دیگران. (۱۳۸۹). انقلاب اطلاعات، امنیت و فناوری های جدید، ترجمه علیرضا طیب، تهران؛ پژوهشکده مطالعات راهبردی.
- ۶- عبدالله خانی، علی. (۱۳۸۳). نظریه‌های امنیت: مقدمه ای بر طرح ریزی دکترین امنیت ملی (۱)، تهران: انتشارات مؤسسه مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.
- ۷- فناوری و قدرت ملی؛ چالش‌ها و راهبردها. (۱۳۸۸). تهران؛ دانشگاه عالی دفاع ملی، انتشارات دانا.
- ۸- قاسمی، علی. (۱۳۸۷). «ویژگی های جنگ ناهمگون (با تاکید بر صحنه نبرد آینده)»، ماهنامه اطلاعات راهبردی، سال ششم، شماره ۶۵.
- ۹- کمیسیون امنیت ملی آمریکا، استراتژی آمریکا در قرن ۲۱. (۱۳۸۰). ترجمه جلال دهمشگی، بابک فرهنگ و ابولقاسم راه چمنی؛ انتشارات موسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران.
- ۱۰- مارتین فن، کرفلد. (۱۳۸۶). بازاندیشی مفهوم جنگ، ترجمه عباداله حیدری، تهران؛ موسسه آموزشی و تحقیقاتی صنایع دفاع، مرکز آینده پژوهی علوم و فناوری.
- ۱۱- محمدی، مصطفی. (۱۳۸۸). «مقایسه جنگ‌های سنتی و نوبین»، ماهنامه اطلاعات راهبردی، سال هفتم، شماره ۸۰.

- ۱۲- والتس، ادوارد.(۱۳۸۶). جنگ اطلاعات؛ اصول و عملیات، ترجمه اکبر رنجبر، حسن حاج قاسم و محمود فخرایی، تهران؛ موسسه آموزشی و تحقیقاتی صنایع دفاعی.
- ۱۳- هرفرید، مونکلر.(۱۳۸۴). جنگ های نوین، ترجمه حسن درگاهی، تهران؛ انتشارات دانشکده فرماندهی و ستاد دوره عالی جنگ سپاه پاسداران.

#### انگلیسی

- 14- Cordesman, Anthony H.(2002). Cyber- Thrests Information Warfare and Critical Infrastructure protection, U.S Homeland; Center for strategic and International Studies.
- 15- Cornish, Edward.(2004). Futuring, The Exploration of the Future, Maryland, published by: World Future Society.
- 16- Fredrick, Henry.(2005). " Hard and Soft Power: The Paradox of Winning the War of Ideas in the 21st Century", US Army War College.
- 17- Gabuer, Alexander.(2001). "print I cold war goes north: Russia and the west begin the race for the arctic region," kommer sant, august 4.
- 18- Gaparro, Rafael(2003). " Concept Information", Annual Review of Information Science and Technology, Vol.37.
- 19- Gerald Fitz, Mary C.(2003). The Russian Military Strategy for Six Generation Warfare, East View Publication.
- 20- Goldman, Emily O.(2003). " Security in the Information Technology Age". Contemporary Security Policy, Vol.24, No.1.
- 21- Griffiths, Martin.(2007). International Relations Theory for the Tewenty - first century: an introduction, London, New York: Roultege.
- 22- Leigh Armistead.(2007). Information warfare, Washington,D.C; Potomac Books, Inc.
- 23- Neilson, Robert.(1997). Sun Tzu and Information Warfare, US National Defense University, NDU Press.
- 24- Peterson, John.(1996). Information Warfare: The Future, in Cyberwar: Security Strategy and Conflict in the Information Age. A lan D. Capen, Douglas H. Dearth, and Thomas Gooden, eds. AFCEA, International Press, Fairfax, VA.
- 25- R.C, Mishra.(2003). Information Warefare and Cyber Security, Authors, press.
- 26- Rattary, Greg, Strategic Warefare in Cyberspace, Cambrdige: The MIT.

- 27- [http://www.cic.nyu.edu/internationalsecurity/docs/NIC\\_final.pdf](http://www.cic.nyu.edu/internationalsecurity/docs/NIC_final.pdf), Global Trends 2025: A Transformed World.
- 28- [http://www.dni.gov/nic/NIC\\_2025\\_project.html](http://www.dni.gov/nic/NIC_2025_project.html).
- 29- Andrew Curry.(2011). 10 Global Trends in 2020, published in 2011, www. The futures company. Com

-۳۰-