DOI: 10.22034/isj.2021.279939.1432

International Studies Journal (ISJ)
Vol. 17, No. 4 (68), Spring 2021
Reseived Date: 2020/9/26
Accept Date: 2021/2/27
Article Type: Original Research
PP: 47-66

فصلنامه مطالعات بین‌المللی
سال ۱۷، شماره ٤ (٦٨)، بهار ١٤٠٠
تاریخ دریافت: ۱۳۹۹/۷/۵
تاریخ پذیرش: ۱۳۹۹/۱۲/۹
نوع مقاله: علمی- پژوهشی
صفحات: ٦٦-٤٧

انقلاب سایبری و تحول مفهوم جنگ اطلاعاتی در عرصه روابط بین‌الملل

دکتر قاسم ترابی* - محمدناصر طاهری‌زاده—

چکیده

جنگ اطلاعاتی جنگ در فضای اطلاعات باهدف آسیب‌زدن به سامانه‌ها، فرآیندها، منابع اطلاعاتی و ساختارهای حیاتی کشور هدف تعریف می‌شود. هدف این جنگ برخلاف گذشته که عمدتاً پیروزی نظامی در جنگ کلاسیک بود، اثرگذاری بر نظام‌های سیاسی، اقتصادی، فرهنگی و اجتماعی، ایجاد کمپین‌های روانی گسترده جهت تضعیف ثبات جامعه و فشار بر یک دولت به‌گونه‌ای است که مطابق با منافع عاملان جنگ اطلاعاتی تصمیم‌گیری و عمل کند. در این راستا، سؤال اصلی مقاله این است که تحت تأثیر انقلاب ارتباطات و اطلاعات و انقلاب سایبری، جنگ اطلاعاتی دچار چه تحولاتی شده است؟ در پاسخ به سؤال فوق، این فرضیه مطرح می‌شود که تحت تأثیر انقلاب ارتباطات و اطلاعات و انقلاب سایبری، جنگ اطلاعاتی از سطح عملیاتی و تاکتیکی به سطح راهبردی گسترش‌یافته و ابعاد سیاسی، اقتصادی، فرهنگی و اجتماعی را دربرگرفته است. روش تحقیق مقاله حاضر توصیفی و تحلیلی است. هدف نهایی مقاله، بحث در مورد تحول در مفهوم و مصداق جنگ اطلاعاتی تحت تأثیر انقلاب ارتباطات و اطلاعات و انقلاب سایبری است. یافته‌های تحقیق نشان می‌دهند، دانش و به‌ویژه دانش سایبری کلید موفقیت در عرصه جنگ اطلاعاتی بهشمار می‌آید.

کلید واژگان

جنگ اطلاعاتی، انقلاب سایبری، اطلاعات غلط عامدانه، اطلاعات غلط غیرعامدانه، پروپاگاندا.

* نویسنده مسئول، دانشیار گروه روابط بین‌الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران.
ایمیل: gh-torabi@iauh.ac.ir
— دانشجوی دکتری گروه روابط بین‌الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران.

Article Link: https://www.isjq.ir/article_132334.html

مقدمه

بدون تردید جنگ اطلاعاتی یا جنگ بر سر کسب اطلاعات از دشمن جهت برتری بر آن، پدیده چندان جدیدی نیست و به شکلی از زمان نخستین جنگ‌ها بین اقوام، جوامع و دولت‌ها، جنگ اطلاعاتی نیز وجود داشته است. به‌عنوان نمونه بیش از دو هزار سال پیش، ژنرال چینی سون تزو[1] در کتاب هنر جنگ[2] اظهار داشت: « در جنگ مهم این است که خودت و دشمن را بشناسی، اگر دشمن و خودت را به‌خوبی بشناسی، در صد جنگ هرگز در معرض خطر نخواهی بود؛ در مقابل اگر از دشمن و از خود بی‌اطلاع باشی، در هر نبردی در معرض خطر خواهی بود». شاید این اولین جمله مکتوب در باب اهمیت اطلاعات و شناخت در جنگ باشد؛ اما دو هزار سال بعد این جمله و تحت تأثیر انقلاب اطلاعات و ارتباطات که اوج آن در انقلاب سایبری قرار دارد، جنگ اطلاعاتی شکل جدیدی به خود گرفته است(Kozloski, 2018:1). در این راستا جنگ اطلاعاتی[3] یکی دیگر از عباراتی است که در کنار عبارات موازی دیگر همچون جنگ سایبری[4]، جنگ‌ترکیبی[5]، جنگ نرم[6]، جنگ معرفتی[7] و امثالهم برای توصیه و مفهوم‌پردازی اشکال نوینی از جنگ و دفاع به کار می‌رود.

بر این مبنا، نباید جنگ اطلاعاتی را پدیده‌ای مجزا از جنگ سایبری، جنگ‌ترکیبی، جنگ نرم و جنگ معرفتی در نظر گرفت، بلکه باید موارد فوق را در کنار و در عرض هم ارزیابی کرد تا شرایط برای درک بهتر از جنگ و دفاع و امنیت در عرصه انقلاب سایبری فراهم شود. لازم به اشاره است که در تمامی موارد فوق که ذیل عنوان جنگ‌های جدید یا نوین مفهوم‌سازی می‌شوند، چند ویژگی کاملاً مشترک وجود دارد. اول اینکه در همه آن‌ها جنبه تخریب فیزیکی یا به تعبیری دیگر جنبه ویرانگری در حداقل قرار دارد و تلاش می‌شود هدف که عمدتاً سیاسی است با حداقل ویرانگری محقق شود. به‌عنوان نمونه تلاش می‌شود در یک جنگ سایبری یا جنگ‌ترکیبی که البته هر دو کاملاً ملازم با جنگ اطلاعاتی هستند، میزان تخریب در حداقل و در آستانه پاسخ مشروع کشور هدف قرار داشته باشد. البته در دیگر اشکال جنگ‌های نوین همچون جنگ نرم یا جنگ اطلاعاتی ممکن است اصولاً تخریبی صورت نگیرد، چراکه هدف بیشتر از

---

[1]. Chinese General Sun Tzu

[2]. The Art of War

[3]. Intelligence War

[4]. Cyber War

[5]. Hybrid War

[6]. Soft War

[7]. Epistemic War

تأسیسات و امکانات، افکار و شهروندان دشمن است؛ بنابراین یکی از مهم‌ترین ویژگی جنگ‌های نوین، نداشتن یا حداقل بودن خسارت فیزیکی است که به همین دلیل برخی آن‌ها را جنگ‌های تمیز[1] نام‌گذاری می‌کنند (Been, 2014:84-112). مسئله دوم نقش برجسته فنّاوری یا به شکل دقیق‌تر انقلاب سایبری در جنگ‌های نوین است. در این راستا باید گفت این فنّاوری است که امکان شکل‌گیری و موفقیت جنگ‌های نوین چون جنگ سایبری، جنگ اطلاعاتی یا جنگ نرم را مهیا نموده است.

بر این اساس اصولاً جنگ‌های نوین جنگ‌هایی بین بازیگران مختلف با سطح فنّاوری و دانش متفاوت هستند. با عنایت به این شرایط آنچه وجه متمایز قطعی جنگ‌های نوین با جنگ‌های نظامی گذشته است، در موضوع انقلاب فنّاوری و به‌خصوص انقلاب سایبری و دانش خلاصه می‌شود. در چنین چارچوبی، جنگ اطلاعاتی یا جنگ بر سر اطلاعات، نمونه‌ای چنین جنگ‌های نوینی است که جنبه فنّاورانه آن کاملاً مشخص و برجسته است. این نوع جنگ چنان تحت تأثیر انقلاب ارتباطات و اطلاعات و به شکل خاص انقلاب سایبری قرارگرفته که از سطح عملیاتی و تاکتیکی فراتر رفته و جنبه راهبردی آن برجسته و وارد عرصه‌های جدیدی شده است. در این راستا، سؤال اصلی مقاله این است که تحت تأثیر انقلاب ارتباطات و اطلاعات و انقلاب سایبری، جنگ اطلاعاتی دچار چه تحولاتی شده است؟ در پاسخ به سؤال فوق، این فرضیه مطرح می‌شود که تحت تأثیر انقلاب ارتباطات و اطلاعات و انقلاب سایبری، جنگ اطلاعاتی از سطح عملیاتی و تاکتیکی به سطح راهبردی گسترش‌یافته و ابعاد سیاسی، اقتصادی، فرهنگی و اجتماعی را دربرگرفته است. در این مقاله تلاش می‌شود این تحولات در مفهوم و مصداق جنگ اطلاعاتی بر اساس روش توصیفی و تحلیلی موردبحث قرار گیرد. درنهایت هدف اصلی مقاله حاضر شناخت تحول در مفهوم و مصداق جنگ اطلاعاتی تحت تأثیر انقلاب ارتباطات و اطلاعات و انقلاب سایبری است.

۱-پیشینه پژوهش

در حوزه جنگ اطلاعاتی منابع بسیار محدودی به زبان فارسی وجود دارد. یکی از این آثار، ترجمه مقاله‌ای با عنوان اطلاعات و جنگ اطلاعات است که بسیاری از مطالب آن به دلیل گذار زمان گویای شرایط امروزی نیستند. این در شرایطی است که تحت تأثیر انقلاب سایبری، جنگ اطلاعاتی با تغییرات بنیادینی مواجه شده است(Niazi and Moradi, 2006:183-193).

در مقاله دیگری با عنوان جنگ اطلاعاتی و نقش آن در جنگ آینده، در باب اهمیت جنگ اطلاعاتی بحث شده است، اما به دلیل قدیمی بودن اثر، انقلاب سایبری و نقش برجسته آن در

[1]. Immaculate War

تغییر مفهوم و ماهیت جنگ اطلاعاتی کمتر مورد توجه قرارگرفته است. درواقع این مقاله بیشتر به بررسی برخی از زوایای جنگ اطلاعاتی پرداخته و کوشیده است تا بعضی از ویژگی‌های این نبرد و قلمروهای منازعاتی آن را موردبحث قرار دهد و کمتر به تحول مفهومی آن عنایت داشته است (Kalhor, 2000: 27-56).

در مقاله دیگری با عنوان گونه‌شناسی نبردهای اطلاعاتی و جنگ سایبری، به مفاهیم اساسی موجود برای درک مفهوم نبرد اطلاعاتی اشاره‌شده است. در این مقاله پس از ارائه مقدمه‌ای در مورد نبرد اطلاعاتی، تاریخچه و تعاریف نبرد اطلاعاتی تبیین و پس‌ازآن به سطوح و راه‌کارهای مورداستفاده درنبرد اطلاعاتی پرداخته شده است. در این مقاله نیز نقش انقلاب سایبری در تحول مفهومی و مصداقی جنگ اطلاعاتی در روابط میان کشورهای جهان مورد توجه قرار نگرفته است (Danesh and Zahedi, 2011: 151-166).

یکی دیگر از آثار مرتبط، مقاله‌ای با عنوان جنگ نرم شبکه‌های ماهواره‌ای در روان‌سازی سیاست خارجی کشورها است که در آن نویسنده بیشتر بر جنگ نرم و نه لزوماً جنگ اطلاعاتی به عنوان ابزاری جهت تأثیرگذاری بر شهروندان تأکید دارد (Doagooyan, 2020: 115-۱۳۰). درنهایت می‌توان به مقاله تأثیر رسانه‌های اصلی بر سیاست خارجی آمریکا در قبال ایران اشاره کرد که در خلال آن به‌شکلی ابعادی از جنگ اطلاعاتی آمریکا علیه جمهوری موردبحث قرارگرفته است، اما به شکل خاص و دقیقی وارد بحث تحول مفهومی جنگ اطلاعاتی نشده است (Ejazi, 2020: 23-45).

۲- چارچوب مفهومی: انقلاب سایبری

بدون تردید یکی از مهم‌ترین ویژگی‌های جهان کنونی، «انقلاب اطلاعات و ارتباطات سایبری»[1] در قالب آن چیزی است که از آن تحت عنوان «انقلاب سایبری»[2] یاد می‌شود. البته درگذشته و به‌خصوص در نیمه دوم قرن بیستم، تکنولوژی‌های ارتباطی و اطلاعاتی در سطوح مختلف وجود داشته‌اند، اما تنها طی دو دهه گذشته است که به دلیل انقلاب صورت گرفته در عرصه سایبر، آنچه از آن تحت عنوان «دهکده جهانی»[3] یاد می‌شود کاملاً محقق شده است. در این زمینه می‌توان به اطلاعات و آمارهای بین‌المللی موجود که مؤید این امر هستند اشاره نمود. بر اساس آمارهای بین‌المللی، استفاده از اینترنت طی یک ده گذشته بیش از چهار برابر شده است.

---

[1]. Cyber Communication Information Revolution

[2]. Cyber Revolution

[3]. Global Village

همچنین در حال حاضر چیزی نزدیک به ۵ میلیارد کاربر اینترنت در سطح جهان فعال هستند (Internet Users, 2021: 1). بر اساس آخرین آمارهای بین‌المللی بیش از ۴۰درصد از جمعیت جهان ارتباط روزانه و مداوم با اینترنت دارند. این در شرایطی هست که در سال ۱۹۹۵ این مقدار چیزی در حدود ۱ درصد بود. افزایش ۳۹ درصدی کاربران اینترنت، یکی از مصادیق آن چیزی است که از آن تحت عنوان انقلاب سایبری یاد می‌شود. به این آمارها باید میزان نفوذ تلفن همراه و تلویزیون‌های دیجیتال و هوشمند را نیز اضافه کرد. بر اساس آخرین آمارهای بین‌المللی که از سوی «اتحادیه بین‌المللی مخابرات»[1] منتشرشده است، چیزی بیش از ۷ میلیارد تلفن همراه در سطح جهان فعال هستند که این امر نشان‌دهنده نفوذ ۹۵,۵ درصدی است. به‌عبارت‌دیگر ۹۵,۵ درصد جمعیت جهان از تلفن همراه استفاده می‌کنند که در حال حاضر ۳,۵ میلیارد آن‌ها هوشمند هستند. ضمن اینکه انقلاب سایبری تغییر و تحولات بنیادینی را در ابعاد مختلف زندگی انسان و به‌تبع آن کشورها ایجاد نموده است؛ به‌واقع تأثیرگذاری انقلاب سایبری بر ابعاد سیاسی، اقتصادی، اجتماعی و فرهنگی در حدی است که می‌توان آن را حتی فراتر از انقلاب صنعتی اول و دوم و حتی فراتر از انقلاب ارتباطات و اطلاعات که خود مقدمه و زمینه انقلاب سایبری بوده است، ارزیابی کرد(Torabi, 2015: 18-29).

به باور برخی سطح و عمق تأثیرگذاری انقلاب سایبری بر جوامع در حدی است که باید قرن بیست‌ویک را قرن سایبری نامید. افزون بر این، فضای سایبر چنان جوامع را تحت تأثیر بنیادین قرار داده است، که دیگر زندگی انسان بدون آن قابل‌تصور نیست. به‌واقع تأثیرگذاری انقلاب سایبری بر زندگی انسان چنان گسترده است که برخی حتی آن را فراتر از اختراع خط و آغاز مدنیت بشر ارزیابی می‌کنند. به‌هرحال این‌یک واقعیت غیرقابل کتمان است که انقلاب سایبری موجی را ایجاد کرده است که هرروز بعد جدیدی از زندگی انسان را دچار تغیر و تحولات گسترده‌ای می‌کند و شکل تازه‌ای به آن می‌دهد (Torabi, 2019: 45-73).

۳- تاریخ تحول مفهوم جنگ اطلاعاتی

از منظر معنایی، جنگ اطلاعاتی به مفهوم گسترده آن از یک‌سو کشمکش بر سر تولید، دست‌کاری و جذب افکار عمومی کشور مقابل بر پایه اطلاعات و ارتباطات است و از سوی دیگر جنگی است که با اعمال نیروی تخریبی در مقیاس وسیع علیه دارایی‌ها و سیستم‌های اطلاعاتی، رایانه‌ها و شبکه‌هایی که از زیرساخت‌های مهم پشتیبانی می‌کنند، اعمال می‌شود. جنگ اطلاعاتی به مفهوم گسترده آن کشمکش بر سر فرایند اطلاعات و ارتباطات است، کشمکشی که با ظهور ارتباطات انسانی آغاز شد (Brian, 2021: 1). ناتو جنگ اطلاعاتی را این‌گونه تعریف

[1]. The International Telecommunication Union

می‌کند: «جنگ اطلاعاتی عملیاتی است که به‌منظور کسب برتری اطلاعاتی نسبت به دشمن انجام می‌شود. این جنگ شامل کنترل فضای اطلاعاتی، محافظت از دسترسی به اطلاعات شخصی، درعین‌حال تلاش در جهت به دست آوردن و استفاده از اطلاعات، تخریب دستگاه‌های اطلاعاتی و ایجاد اختلال در جریان اطلاعات دشمن است». جنگ اطلاعاتی پدیده جدیدی نیست، اما شامل عناصر ابتکاری درنتیجه توسعه فناوری است که منجر به انتشار سریع و وسیع‌تر اطلاعات می‌شود (Information Warfare. 2005: 1). وزارت دفاع آمریکا جنگ اطلاعاتی را چنین تعریف می‌کند:«اقدامات انجام‌شده برای دستیابی به برتری اطلاعاتی نسبت به دشمن با تأثیرگذاری بر اطلاعات، فرآیندهای مبتنی بر اطلاعات، سیستم‌های اطلاعاتی و شبکه‌های مبتنی بر رایانه دشمن، درحالی‌که از اطلاعات شخصی، فرآیندهای مبتنی بر اطلاعات، سیستم‌های اطلاعاتی و شبکه‌های مبتنی بر رایانه خود دفاع می‌شود». در تعریف تکمیلی وزارت دفاع آمریکا تأکید می‌کند که جنگ اطلاعاتی «توانایی جمع‌آوری، پردازش، انتشار جریان بی‌وقفه اطلاعات برای دستیابی یا ارتقا اهداف خاص نسبت به یک دشمن خاص است، درحالی‌که دسترسی به این توانایی‌ها برای دشمن انکار می‌شود (Ramlee, 2005: 1-2). به تعبیری دیگر جنگ اطلاعاتی جنگ هرچیزی مرتبط با فریب دشمن است. این جنگ شامل اطلاعات، فرایندهای اطلاعاتی، زیرساخت‌های اطلاعاتی، افراد و رهبران است. از طرف دیگر جنگ اطلاعاتی همچنین تلاشی است جهت تهیه دقیق و به‌موقع اطلاعات موردنیاز رهبران برای کمک به آن‌ها در فرایندهای تصمیم‌گیری (Ramlee, 2005: 3).

نیروی هوایی آمریکا جنگ اطلاعاتی را این‌گونه تعریف می‌کند:«جنگ اطلاعاتی غالباً یک اصطلاح موردبحث است و درواقع فاقد تعریف مشترک مورد تائید است؛ اما برای آمریکا، جنگ اطلاعاتی به‌عنوان فعالیت‌هایی است که عناصر اطلاعاتی، نظارتی و شناسایی، عملیات فضای مجازی، جنگ الکترومغناطیسی و عملیات اطلاعاتی را برای دستیابی به نتایج در زمان جنگ و صلح هماهنگ می‌کند. امروز نیروی هوایی آمریکا جنگ اطلاعاتی را استفاده از توانایی‌ها و ظرفیت‌های نظامی در محیط اطلاعاتی جهت تأثیر عمدی بر رفتار عوامل و سیستم اطلاعاتی دشمن توصیف می‌کند (Gagnon, 2020: 5). ژنرال تیموتی هوگ[1] فرمانده شانزدهم نیروی هوایی یا همان سازمان تازه تأسیس جنگ اطلاعات نیروی هوایی[2] دراین‌باره می‌گوید: «یکی از بارزترین نمونه‌هایی که نشان می‌دهد ارتش چگونه می‌خواهد با استفاده از جنگ اطلاعاتی دشمنان را شکست دهد، تلاش در جهت این است که بفهمد دشمن چه هدفی دارد و چه توانایی‌هایی جهت تحقق آن اهداف دارد. بر این اساس جنگ اطلاعاتی می‌تواند انتزاعی باشد،

[1]. Gen. Timothy Haugh

[2] .Information Warfare Organization

جنگی که ترکیبی از امکانات فضای سایبر، اطلاعات، جنگ الکترونیکی، عملیات اطلاعاتی، عملیات روانی یا فریب نظامی است. هدف نهایی از این اقدامات تأثیرگذاری بر محیط اطلاعاتی یا تغییر طرز فکر دشمن هست»(Mark, 2020: 1).

برخی دیگر جنگ اطلاعاتی را در اصل همان اطلاعات نظامی می‌دانند که در معنای محدود به معنای جنگ اطلاعاتی بین ارتش کشورهای متخاصم است. اطلاعات نظامی شامل کلیه فعالیت‌هایی است که به جمع‌آوری، تجزیه‌وتحلیل و انتشار اطلاعات برای واحدهای نظامی و تصمیم‌گیرندگان اختصاص داده می‌شود. اطلاعات نظامی به اطلاعات انسانی[1] یا اطلاعات فنی شامل اطلاعات تصویری[2] و اطلاعات الکترونیک[3] تقسیم می‌شود. فعالیت‌های اطلاعاتی چه در زمان صلح و چه در زمان جنگ در سطوح تاکتیکی، عملیاتی و استراتژیک انجام می‌شود (Military Intelligence Training, 2021).

اطلاعات نظامی یک‌رشته نظامی است که با استفاده از روش‌های جمع‌آوری و تجزیه‌وتحلیل اطلاعات، فرماندهان را در تصمیم‌گیری‌ها کمک می‌کند. این هدف با ارائه ارزیابی داده‌ها از طیف وسیعی از منابع، به سمت نیازهای مأموریت فرماندهان یا پاسخ به سؤالات ویژه به‌عنوان بخشی از برنامه‌ریزی عملیاتی محقق می‌شود. برای ارائه تجزیه‌وتحلیل ابتدا نیازهای اطلاعاتی فرمانده مشخص می‌شود، سپس در جمع‌آوری، تجزیه‌وتحلیل و انتشار اطلاعات گنجانده می‌شود. مناطق موردمطالعه ممکن است شامل محیط عملیاتی، نیروهای متخاصم، کشورهای دوست و بی‌طرف، جمعیت غیرنظامی در منطقه‌ای از عملیات جنگی و سایر مناطق موردعلاقه باشد. فعالیت‌های اطلاعاتی در همه سطوح، از تاکتیکی تا استراتژیک، در زمان صلح و دوره انتقالی جنگ و در طول جنگ انجام می‌شود. فراتر از اطلاعات نظامی، در اطلاعات استراتژیک به موضوعات گسترده‌ای مانند اقتصاد، تحلیل سیاسی، توانایی‌های نظامی و اهداف دول خارجی و به‌طور فزاینده بازیگران غیردولتی همچون تروریست‌ها پرداخته می‌شود. چنین اطلاعاتی ممکن است علمی، فنی، تاکتیکی، دیپلماتیک یا جامعه‌شناختی باشد، اما این تغییرات در ترکیب با واقعیت‌های شناخته‌شده در مورد منطقه موردبحث مانند جغرافیا، جمعیت و ظرفیت‌های صنعتی مورد تجزیه‌وتحلیل قرار می‌گیرد. اطلاعات استراتژیک به‌صورت رسمی به‌عنوان اطلاعات موردنیاز برای شکل‌گیری سیاست‌ها و برنامه‌های نظامی در سطح ملی و بین‌المللی تعریف می‌شود و با سطح استراتژیک جنگ مطابقت دارد (Rolington, 2013).

برخی دیگر از کارشناسان جنگ اطلاعاتی را به سه دسته تقسیم می‌کنند. اول جنگ برای

---

[1]. Human Intelligence

[2]. Technical Intelligence – Mainly Imagery Intelligence

[3]. Electronic Intelligence

اطلاعات که به معنای به دست آوردن اطلاعات در مورد ابزارها، ظرفیت‌ها و استراتژی‌های دشمن است. دوم جنگ علیه اطلاعات که به معنای حفاظت از سامانه‌های اطلاعاتی هم‌زمان با ایجاد اختلال یا نابودسازی منابع ذخیره اطلاعات دشمن است؛ و سوم جنگ به‌وسیله اطلاعات که به معنای تولید اطلاعات غلط یا فریبنده به‌گونه‌ای است که منجر به سلطه اطلاعاتی و رسانه‌ای شود. شاید به‌روزترین تعریف از جنگ اطلاعاتی توسط دولت روسیه مطرح‌شده باشد که البته این دولت در این عرصه یکی از موفق‌ترین‌ها نیز محسوب می‌شود. دولت روسیه جنگ اطلاعاتی را این‌گونه تعریف می‌کند: «منازعه میان دو دولت یا بیشتر، در فضای اطلاعات باهدف آسیب زدن به سامانه‌ها، فرآیندها و منابع اطلاعاتی و ساختارهای حیاتی و غیر آن؛ اثرگذاری بر نظام‌های سیاسی، اقتصادی و اجتماعی؛ ایجاد کمپین‌های روانی گسترده علیه یک ملت جهت تضعیف ثبات جامعه و حکومت و فشار به یک دولت به‌گونه‌ای که مطابق با منافع مخالفانش تصمیم‌گیری کند» (Russia's New Strategy: Information Warfare and Combined Warfare, 2017: 1). همان‌گونه که تعریف فوق نشان می‌دهد، ازنظر دولت روسیه جنگ اطلاعاتی فراتر از حوزه نظامی و فراتر از تلاش برای تخریب سامانه‌های اطلاعاتی دشمن، تمامی عرصه‌ها و ابعاد کشور دشمن را هدف تهاجم خود قرار می‌دهد.

همان‌گونه که گفته شد، روسیه یکی از پیشروترین کشورها در عرصه جنگ اطلاعاتی و البته گسترش معنا و مفهوم آن محسوب می‌شود. در گزارشی در باب جنگ اطلاعاتی روسیه آمده است: «روسیه تنها تهدیدی اطلاعاتی برای اروپا و ایالات‌متحده نیست، بلکه روسیه دارای یک استراتژی جهانی است که به دلیل پیچیدگی هر منطقه از جهان را به درجات مختلف تحت تأثیر قرار می‌دهد. رویکرد روسیه در جنگ اطلاعاتی جامع‌نگر است و شامل حملات سایبری و عملیات اطلاعاتی به‌عنوان عناصر منسجمی می‌شود که هم‌زمان برای دستیابی به اهداف سیاست خارجی روسیه کار می‌کنند (Cunningham, 2020: 1). علاوه بر این، روسیه در جنگ اطلاعاتی نه‌تنها به دنبال تضعیف نیروهای مسلح دشمن است، بلکه همچنین بر درک جمعیت هدف تأثیر می‌گذارد، به‌گونه‌ای که منافع روسیه را تأمین کند. برخلاف عملیات سایبری، عملیات اطلاعاتی بسیار قدیمی است که کرملین مدت‌هاست برای تحقق اهداف خود از آن استفاده می‌کند. رهبران شوروی خیلی زود ارزش اطلاعات و چگونگی استفاده از آن برای تأثیرگذاری بر توده مردم در داخل و خارج را درک کردند؛ متعاقباً، فدراسیون روسیه توانسته است با استفاده از اینترنت، اثربخشی جنگ اطلاعاتی را با هزینه کم افزایش دهد (Arampatzis and Cobaugh, 2018). در این راستا رسانه‌هایی که توسط دولت روسیه پشتیبانی می‌شوند و توسط ترول‌ها[1] و ربات‌های روسی

[1]. Internet Trolls

پشتیبانی می‌شوند، به یکی از عناصر اصلی جنگ اطلاعاتی روسیه تبدیل شده‌اند. آن‌ها با تضعیف سیستم بین‌المللی پس از جنگ سرد که تحت سلطه غرب و نهادهای دموکراتیک جهانی است، برای ترویج نسخه‌ای از وقایع جهان که به اهداف سیاست خارجی روسیه نزدیک است، کار می‌کنند. آن‌ها به تقویت افراط‌گرایی در هر دو طرف طیف سیاسی یعنی چپ و راست در غرب کمک کرده و به روش‌های هدفمند برای کمک به عملیات خارجی روسیه کارکرده‌اند (Troianovski, Warrick, 2018: 1).

با عنایت به تعاریف فوق می‌توان گفت جنگ اطلاعاتی تحت تأثیر انقلاب ارتباطات و اطلاعات و همچنین به شکل خاص تحت تأثیر انقلاب سایبری، دچار قبض و بسط مفهومی شده است. اول اینکه انقلاب‌های ارتباطات و اطلاعات و انقلاب سایبری، جنگ اطلاعاتی را از حوزه عملیاتی و تاکتیکی نظامی به حوزه‌های راهبردی گسترش داده و امروز دیگر فقط حوزه نظامی نیست که درگیر جنگ اطلاعاتی است، بلکه دولت‌ها تمامی عرصه‌های نظامی، سیاسی، اقتصادی، فرهنگی و اجتماعی و حتی ادراکی و شناختی را هدف جنگ اطلاعاتی خود قرار می‌دهند؛ بنابراین جنگ اطلاعاتی هم جنبه استراتژیک پیداکرده است و هم ابعاد مختلف را هدف قرار می‌دهد. نکته دوم همراهی و ملازمت جنگ اطلاعاتی با انواع دیگر جنگ‌های نوین ازجمله جنگ سایبری و جنگ‌ترکیبی است که اجرای هم‌زمان آن‌ها، باعث هم‌افزایی قدرت کشور مهاجم و آسیب‌پذیری بیشتر کشور مدافع می‌شود. نکته قابل‌توجه این است که چنین جنگ‌های نوینی چنان در حوزه مفهومی و مصداقی به هم نزدیک هستند که گاهی تمایز آن‌ها از همدیگر امکان‌پذیر نیست. در این راستا برخی از کارشناسان تلاش می‌کنند از عبارت جنگ‌ترکیبی برای همه موارد فوق استفاده کنند و جنگ‌ترکیبی را عملاً ترکیبی از جنگ اطلاعاتی و سایبری معرفی کنند که البته چندان با واقعیات و مصادیقی چون جنگ‌ترکیبی روسیه علیه اوکراین منافاتی ندارد.

لازم به اشاره است که جنگ‌ترکیبی همچون جنگ اطلاعاتی تمایز میان آنچه بخشی از میدان جنگ است و آنچه بخشی از آن نیست و یا به تعبیری تمایز بین جنگ و صلح را از بین می‌برد. جنگ‌ترکیبی هم چندوجهی است و هم در یک‌زمان در سطوح چندگانه به کار گرفته می‌شود که سطوح سنتی جنگ شامل تاکتیک، عملیات و راهبرد را فشرده ساخته و بدین ترتیب سرعت را در سطوح راهبردی و عملیاتی بیش از توانایی انجام یک بازیگر متعارف بالا می‌برد. در یک جنگ‌ترکیبی فضاهای فیزیکی سنتی مانند زمین، دریا، هوا و فضا به نحو فزاینده‌ای با فضاهای اجتماعی و برساخته مانند فضای سیاسی، اقتصادی، فرهنگی، اطلاعاتی و سایبری و از همه مهم‌تر فضاهای شناختی و روانی و البته اطلاعاتی پیوند می‌خورند؛ درنتیجه ضرورت کاربست نیروی

(ادامه از صفحه قبل) ترول به افرادی گفته می‌شود که با رفتار مخرب در فضای وب به دنبال جلب نظر کاربران، ایجاد تشنج و بیان مطالب محرک و توهین‌آمیز هستند. ترول‌ها، افرادی هستند که در اتاق‌های گفتگو، تالارها،وب‌نوشت‌ها یا تارنماهای کاربر-محور، پیام‌هایی ارسال می‌کنند که حاوی مطالب ناراحت‌کننده یا جنجال‌برانگیز است.

نظامی سخت را کاهش می‌دهد. در این راستا، به‌جای اجبار دشمن به تسلیم به‌وسیله نابود کردن توانمندی‌های نظامی لازم برای مقاومت، میدان اصلی جنگ در فضاهای شناختی جمعیت‌های کلیدی داخلی و بین‌المللی قرار می‌گیرد و دشمن را وادار به تسلیم یا دادن امتیاز می‌کند (Mumford, 2020: 3).

٤- تکنیک‌های جنگ اطلاعاتی و مزیت‌ها و چالش‌های آن

در این بخش تکنیک‌های جنگ اطلاعاتی و مزیت‌ها و چالش‌های آن مورد بررسی قرار می‌گیرد.

٤-١- تکنیک‌های جنگ اطلاعاتی

در جنگ اطلاعاتی از دسته‌های مختلف اطلاعات، روش‌ها و تکنیک‌های متنوع فریب، دروغ، شایعه‌پراکنی، وارونه جلوه دادن واقعیت، بزرگنمایی و کوچک‌نمایی استفاده می‌شود، اما تحت تأثیر انقلاب ارتباطات و اطلاعات و به‌ویژه انقلاب سایبری حوزه‌های جدیدتری چون پروپاگاندا،[1] اطلاعات غلط غیرعامدانه یا میس‌اینفورمیشن[2] اطلاعات غلط عامدانه یا دیس اینفورمیشن[3] و مل‌اینفورمیشن[4] به آن‌ها اضافه شده است که در ادامه موارد فوق به‌تفصیل مورد بحث و بررسی قرار می‌گیرند.

٤-١-١- مدیریت ادراک

مدیریت ادراک[5] یکی از تکنیک‌های اصلی در جنگ اطلاعات است که طی آن تلاش می‌شود ادراک شهروندان و رهبران کشور هدف در راستای اهدافی مدیریت شود. ادراک فرایندی است که توسط آن افراد ورودی‌های حواس خود را انتخاب می‌کنند، سازمان می‌دهند و تفسیر می‌کنند تا به جهان اطراف خود معنا دهند. در این راستا مدیریت ادراک عملی است که اطمینان حاصل می‌کند پیامی که می‌خواهید ارسال کنید توسط افراد یا گروه‌های خاصی که می‌خواهید به آن‌ها برسد قابل‌درک است. مدیریت ادراک همچنین به معنای تأثیرگذاری بر چگونگی تفسیر دیگران است. پاسکال کومبلس سیگل[6] در باب اهمیت مدیریت ادراک و کم‌توجهی به آن در ارتش آمریکا می‌نویسد: «مدیریت ادراک فرزند ناتنی عملیات اطلاعاتی

---

1. Propaganda
2. Misinformation
3. Disinformation
4. Malinformation
5. Perception Management
6. Pascale Combelles Siegel

ارتش[1] است؛ به این دلیل که فناوری عملیات اطلاعاتی ارتش را تا حدی کنترل کرده است که درنتیجه این امر تأکید قبلی آن بر مدیریت ادراک به نقش ثانویه تبدیل‌شده است. این در شرایطی است سایر کشورها باکمال میل این فرزندخوانده را به‌عنوان فرزند خود پذیرفته‌اند. به‌هرحال اینکه سایر کشورها چقدر این فرزند ناتنی را به‌خوبی پرورش می‌دهند، تفاوت بین موفقیت و شکست را ایجاد می‌کند. مدیریت ادراک معمولاً مراحلی دارد. در مرحله اول باید مشخص شود مخاطب جنگ چگونه ادراکی به‌خصوص در مورد ما دارد. به تعبیری دیگر فکر می‌کنید چگونه ادراک می‌شوید؟ بنابراین ابتدا باید به‌روشنی تعریف شود که فکر می‌کنید دیگران چگونه شما را درک می‌کنند.

لازم به اشاره است که افراد، شرکت‌ها، ارتش‌ها و دولت‌ها که در تحلیل نهایی انسان هستند، معمولاً تعصباتی را تجربه می‌کنند. این به معنای نسبت دادن موفقیت به عوامل داخلی و عدم موفقیت به موانع خارجی است. در مرحله دوم باید روشن شود یک ارتش یا دولت چگونه می‌خواهد درک شود؟ چه تفاوتی بین ادراک از خود و درک واقعی از شما وجود دارد؟ اگر این دو باهم مطابقت داشته باشند، به این معنی نیست که نباید کاری انجام داد. این بدان معنی است که این درک باید تقویت شود. اگر باهم مطابقت نداشته باشند، این بدان معنا نیست که مشکل جدی وجود دارد، بلکه باید تلاش را جدی‌تر کرد (Khan, 2015: 1). لازم به اشاره است که مدیریت ادراک اصطلاحی است که توسط ارتش ایالات‌متحده ایجادشده است. وزارت دفاع آمریکا آن را چنین تعریف می‌کند: «اقداماتی برای انتقال یا انکار اطلاعات و شاخص‌های منتخب به مخاطبان خارجی برای تأثیرگذاری بر احساسات، انگیزه‌ها و استدلال‌های عینی آن‌ها و همچنین تحت تأثیر قراردادن سیستم‌های اطلاعاتی و رهبران در همه سطوح، برای تأثیرگذاری بر تخمین‌های رسمی و درنهایت منجر به رفتارها و سیاست خارجی و اقدامات رسمی مطلوب». مدیریت ادراک پیش‌بینی واقعیت، امنیت عملیات، پوشش و فریب و عملیات روانی را باهم ترکیب می‌کند. اگرچه عملیات مدیریت ادراک درصحنه بین‌المللی انجام می‌شود، اما استفاده از فن‌های مدیریت ادراک به بخشی از سیستم‌های اصلی مدیریت اطلاعات حتی در عرصه داخلی نیز تبدیل شده‌اند. به‌عنوان نمونه موارد بسیاری وجود دارد که ایالات‌متحده آمریکا درگیر مدیریت ادراک داخلی بوده است. به‌عنوان‌مثال می‌توان به ممنوعیت عکاسی از تابوت‌های سربازان آمریکایی اشاره کرد که هنگام ورود به ایالات‌متحده به‌صورت عمده تخلیه می‌شوند. در طول جنگ ویتنام نیز پنتاگون برای جلب حمایت بیشتر مردم از جنگ، در مورد تهدیدهای کمونیست‌ها علیه ایالات‌متحده اغراق می‌کرد. همچنین در سال‌های پیش از حمله به عراق در سال ۲۰۰۳، ایالات‌متحده از روش‌های مدیریت ادراک برای ترویج این باور که سلاح‌های کشتارجمعی در عراق تولید

[1]. Military Information Operations (IO)

می‌شوند استفاده کرد و اینکه دولت عراق به تروریست‌های القاعده مسئول حملات ۱۱ سپتامبر ۲۰۰۱ کمک کرده است. لس‌آنجلس تایمز در مقاله‌ای گزارش داد که پنتاگون به‌طور مخفیانه به روزنامه‌نگاران عراقی پول داده است تا داستان دلاوری‌های سربازان آمریکایی را منتشر کنند. در این گزارش آمده است که داستان‌های یک‌طرفه و دروغ به‌عنوان گزارش‌های بی‌طرفانه تولیدشده توسط روزنامه‌نگاران مستقل ارائه شده است (Kapoor, 2009: 1).

٤-١-٢- پروپاگاندا

پروپاگاندا در لغت به معنای تبلیغات است و در اصطلاح اطلاعاتی عبارت است از کوشش برای ترویج نظرات خاص سیاسی از طریق گزارش‌های غیرواقعی به‌قصد تأثیر گذاشتن بر ذهن مخاطب و ترغیب به رفتار خاص. این عمل به‌وسیله دولت‌ها، احزاب و گروه‌ها صورت می‌گیرد و هدف اصلی آن جهت‌دهی به افکار عمومی و القاء اندیشه‌ها و افکار خاص و مقبولیت عملکردها در میان توده‌های مردم و افکار جهانیان است. در نیمه اول قرن بیستم، نازی‌ها و فاشیست‌ها از این واژه در تبیین کنترل اجتماعی و مشروعیت دادن به حکومت بهره می‌بردند. در دوران جنگ جهانی دوم نیز دولت‌های درگیر جنگ با به‌کارگیری ابزارهای مختلف تبلیغی جهت نیل به اهداف سیاسی خود همچون تقویت روحیه مردم و بسیج نیروها و تضعیف روحیه دشمن تلاش می‌کردند. از همین زمان بود که پروپاگاندا به معنای تبلیغات سیاسی رواج یافت. در دوران جنگ سرد دو بلوک شرق و غرب به‌طور بسیار گسترده و پیشرفته‌ای از تبلیغات جهت گسترش حوزه نفوذ خود علیه جبهه مقابل استفاده کرده‌اند. البته پروپاگاندا در جهان کنونی و در زمانه‌ای که عصر انفجار اطلاعات خوانده می‌شود، در سیاست جایگاه ویژه‌ای پیدا کرده است. گسترش وسایل ارتباط‌جمعی و رسانه‌های گوناگون، تبلیغات سیاسی را پیچیده و روزافزون کرده است. از همین رو دولت‌ها، گروه‌ها و احزاب سیاسی در تلاش هستند با به‌کارگیری همهٔ ابزارهای تبلیغی همچون مطبوعات، فرستنده‌های قوی، سایت‌های اینترنت، سخنرانی‌ها و سینما، ایده‌ها و اندیشه‌های خود را به مخاطبین انتقال دهند (What is Propaganda?, 2017).

٤-١-٣- اطلاعات غلط غیرعامدانه و عامدانه

بدون تردید یکی از مهم‌ترین تهدیدات امنیتی فراگیر برای افراد، سازمان‌ها و البته دولت‌ها که البته هنوز ابعاد و عمق تهدیدزای آن چندان آشکارنشده است، مسئله رو به گسترش اخبار جعلی[1] در فضای سایبر و به‌خصوص در شبکه‌های اجتماعی عامه‌پسند است. اخبار جعلی حداقل شامل سه دسته اطلاعات می‌شود. این سه دسته شامل اطلاعات غلط غیرعامدانه یا میس‌اینفورمیشن[2]

[1] Fake News

[2] Misinformation

اطلاعات غلط عامدانه یا دیس‌اینفورمیشن[1] و مل‌اینفورمیشن[2] می‌شود. اطلاعات غلط غیرعامدانه یا میس‌اینفورمیشن، گسترش ناخواسته اطلاعات غلط است که تقریباً همه افراد روزانه با آن درگیر هستند، چراکه بخش مهمی از اطلاعات موجود در شبکه‌های مجازی عملاً نادرست هستند و افراد ناخواسته آن‌ها را می‌بینند و به اشتراک می‌گذارند؛ بنابراین به شکلی همه افرادی که در شبکه‌های اجتماعی حضور دارند، حتی آن‌هایی که حضور حداقلی دارند به اشکال مختلف درگیر اطلاعات غلط غیرعامدانه هستند. به‌عنوان‌مثال می‌توان به ترول‌های اینترنتی[3] اشاره کرد که به گسترش نظریه‌های توطئه بی‌اساس یا کلاه‌برداری از طریق رسانه‌های اجتماعی دامن می‌زنند. برخلاف میس‌اینفورمیشن، در اطلاعات غلط عامدانه یا دیس‌اینفورمیشن، مهاجمان عمداً و برای تأمین هدف خاص اخبار دروغ را منتشر می‌کنند. به‌عنوان‌مثال می‌توان به گسترش اخبار دروغ در رسانه‌ها و یا انتشار اطلاعات محرمانه و سری قبل از انتشار رسمی آن‌ها جهت ضربه زدن به دولت یا بازیگرانی خاص اشاره کرد(Defense Primer: Information Operations, 2020: 1-3). به تعبیری بهتر در دیس‌اینفورمیشن، مهاجم تلاش می‌کند اطلاعات نادرست و مخرب را به‌طور عمدی برای ایجاد آسیب به اشتراک گذارد. بهترین نمونه از تهاجم با اخبار جعلی عامدانه، نقش روسیه در انتخابات آمریکا در سال ۲۰۱۶ یا نقش آن در مسئله برگزیت و رشد راست افراطی در کشورهایی اروپایی است (Tanner, 2020: 1-13).

بر اساس مدارک و شواهد موجود، عوامل روسیه در کمپین‌های گسترده ایجاد و گسترش اخبار جعلی، نقش مهمی در انتخابات آمریکا، برگزیت و رشد راست افراطی در کشورهایی اروپایی داشته و دارند. درنهایت مل‌اینفورمیشن اطلاعات کاملاً درستی است که در زمان مشخص با هدف تأثیرگذاری در جهت تأمین منافع از آن استفاده می‌شود. بهترین نمونه این امر، نفوذ هکرهای روس به ایمیل خانم کلینتون و انتشار آن‌ها جهت تخریب چهره وی در خلال انتخابات ریاست جمهوری ۲۰۱۶ است. در این رسوایی هکرهای روس اطلاعات درست و واقعی را منتشر کردند، اما زمان و نحوه انتشار آن با هدف تخریب چهره خانم کلینتون و بالابردن شانس رقیب وی دونالد ترامپ بود؛ بنابراین در مل‌اینفورمیشن مهاجم اخبار واقعی و صحیح را با هدف تأمین منافع خود و ضربه زدن به دیگری دنبال می‌کند. لازم به اشاره است که مل‌اینفورمیشن در سطح جامعه می‌تواند برای افراد و خانواده‌ها و به تعبیری شهروندان عادی مسائل و مشکلات جدی ایجاد کند، کما اینکه تا به امروز نیز همین‌گونه بوده است. به‌عنوان نمونه به دست آوردن و پخش محتوای خصوصی زندگی افراد عادی یا سازمان و شرکت‌ها جهت ضربه زدن به آن‌ها در همین قالب مل‌اینفورمیشن قرار می‌گیرد(Staats, 2021: 1).

---

[1]. Disinformation

[2]. Malinformation

[3]. Internet Trolls

لازم به اشاره است که دشمنان از فن‌های مختلفی برای گسترش اطلاعات نادرست استفاده می‌کنند. معمولاً بیشتر آن‌ها از سیستم‌عامل‌های رسانه‌های اجتماعی که برای تبلیغ محتوای محبوب طراحی‌شده‌اند و احساسات شدیدی را برمی‌انگیزند بهره می‌برند. اطلاعات نادرست با ویژگی‌های ویروسی اغلب مبتنی بر الگوهای رفتاری و فیلم‌های کوتاه است که به‌طور گسترده در برنامه‌های پیام بسته[1]مانند فیس‌بوک و واتس‌اپ به اشتراک گذاشته می‌شود. نمایندگان اطلاعات نادرست همچنین می‌توانند وب‌سایت‌های جعلی و یا حساب‌های جعلی در رسانه‌های اجتماعی[2] ایجاد کنند تا پیام‌های خود را میزبانی کنند، این تاکتیکی معروف است که به آن تبلیغ محاسباتی[3] می‌گویند. همچنین افراد می‌توانند در گروه‌های موجود فیس‌بوک یا واتس‌اپ عضو شوند و محتوای نادرست را به‌طور گسترده به اشتراک گذارند. این روند جعلی گاهی اوقات به حدی می‌رسد که توسط رسانه‌های خبری اصلی و سنتی نیز جذب می‌شود. ضمن این‌که کسانی که اطلاعات نادرست را گسترش می‌دهند به‌طور فزاینده‌ای از هوش‌مصنوعی برای ایجاد روش‌های پیچیده‌تر برای انجام این کار استفاده می‌کنند، ازجمله ایجاد حساب‌های ربات واقع‌گرایانه‌تر و فیلم‌های جعلی که برخی محققان قبلاً آن را جدی‌ترین تهدید نامیده‌اند (Tanner, 2020: 1-13).

٤-٢- مزیت‌ها و چالش‌های جنگ اطلاعاتی

جنگ اطلاعاتی دارای مزیت‌های گسترده و البته چالش و مشکلات متنوعی است. بر این اساس این نوع جنگ هم ابزاری کارآمد و البته کم‌هزینه جهت تحقق اهداف سیاسی است و هم می‌تواند به دلیل ماهیت پویا منشأ تهدیدات امنیتی باشد. به تعبیری دیگر جنگ اطلاعاتی در جنبه آفندی کارآمد و مشکل‌گشا هست، ولی در صورت عدم آمادگی در برابر آن می‌تواند کاملاً تهدیدآفرین باشد. درواقع به همین دلیل است که ویلیام پری[4]یکی از باتجربه‌ترین وزیران دفاع سابق آمریکا در باب جنگ اطلاعاتی می‌گوید:« ما در عصری زندگی می‌کنیم که توسط اطلاعات هدایت می‌شود. پیشرفت‌های فنی در حال تغییر چهره جنگ و چگونگی آماده شدن برای جنگ هستند»(Molander, Riddile and Wilson, 1996: 1). بر این اساس در ادامه مزیت‌ها و چالش‌های جنگ اطلاعاتی موردبحث و بررسی قرار می‌گیرند.

٤-٢-١- کم هزینه‌بودن

برخلاف فن‌آوری‌های سنتی سلاح، توسعه تکنیک‌های مبتنی بر اطلاعات نیازی به منابع مالی قابل‌توجه ندارد. در این نوع جنگ، تخصص سیستم‌های اطلاعاتی و دسترسی به شبکه‌های مهم

---

1. Closed Messaging Apps
2. Fake Social Media Accounts
3. Computational Propaganda
4. William Perry

تنها پیش‌نیازها هستند. ضمن اینکه شبکه‌های به‌هم‌پیوسته ممکن است نه‌تنها توسط دولت‌ها بلکه توسط بازیگران غیردولتی ازجمله گروه‌های غیردولتی و حتی افراد موردحمله و اختلال قرار گیرد. دشمنان بالقوه نیز می‌توانند از طیف گسترده‌ای از توانایی‌ها برخوردار باشند؛ بنابراین تهدید منافع دولت‌ها می‌تواند به‌طور فراوانی افزایش یابد و با توسعه سیستم‌های پیچیده‌تر و گسترش تخصص‌های لازم، تأمین امنیت به‌شدت مشکل شود. برخی از کارشناسان بر این باور بودند که می‌توان با محروم کردن دسترسی آسان به شبکه‌ها و سیستم‌های کنترل از طریق بهره‌برداری از تکنیک‌های جدید رمزگذاری نرم‌افزار، ورود عوامل تهدیدزا را به‌شدت مشکل کرد؛ اما واقعیت این است که این کار ممکن است برخی از تهدیدات را کاهش دهد، اما همه مشکلات را حل نمی‌کند. این امر همچنین باعث افزایش دشواری در اطلاعات استراتژیک و تاکتیکی در مقابل مهاجمان استراتژیک جنگ اطلاعاتی می‌شود (Molander, Riddile and Wilson, 1996:1).

٤-٢-٢- درهم ریختن مرزهای سنتی مفاهیم

جنگ اطلاعاتی تمایزهای سنتی مانند منافع عمومی در برابر منافع خصوصی، رفتارهای جنگ‌طلبانه در مقابل رفتارهای جنایت‌کارانه و مجرمانه و مرزهای جغرافیایی و مرزهای بین ملت‌ها که به‌طور تاریخی تعریف‌شده‌اند را به‌هم‌ریخته است. درواقع با توجه به تعداد گسترده‌ای از دشمنان، سلاح‌ها و استراتژی‌های احتمالی، تمایز بین تهدیدات و اقدامات مبتنی بر جنگ اطلاعاتی خارجی و داخلی دشوارتر شده است. معمولاً در چنین جنگ‌های چندان آشکار نیست چه کشوری توسط چه کسانی موردحمله قرار می‌گیرد، یا چه کسی مسئول حمله است. پیامد دیگر این پدیده پیچیده شدن و از بین رفتن تمایزهای واضح بین سطوح مختلف اقدامات خشونت‌بار، از جنایت تا جنگ است. با توجه به این پیچیدگی، دولت‌های مهاجم می‌توانند از انواع سنتی‌تر اقدامات نظامی یا تروریستی چشم‌پوشی کنند و در عوض از افراد یا سازمان‌های جنایی فراملی برای انجام عملیات استراتژیک استفاده کنند (Molander, Riddile and Wilson, 1996:1).

٤-٢-٣- آسان‌تر کردن مدیریت ادراک

تکنیک‌های جدید مبتنی بر اطلاعات ممکن است به‌طور فراوانی قدرت فریب و فعالیت‌های دست‌کاری تصویر را افزایش دهند و بدین ترتیب تلاش دولت‌ها برای ایجاد پشتیبانی سیاسی از ابتکارات مربوط به امنیت را به‌طور چشمگیری پیچیده‌تر کنند. به تعبیری دیگر جنگ اطلاعات، مدیریت امنیتی دولت‌ها را به‌شدت مشکل نموده است. به‌عنوان‌مثال، گروه‌های سیاسی و سایر سازمان‌های غیردولتی می‌توانند از اینترنت برای حمایت سیاسی استفاده کنند. بعلاوه این احتمال به وجود آمده که واقعیات را بتوان از طریق تکنیک‌های چندرسانه‌ای دست‌کاری و به‌طور گسترده منتشر کرد. همچنین درنتیجه اقدامات دشمن، ممکن است توانایی ایجاد و حفظ حمایت داخلی از اقدامات سیاسی بحث‌برانگیز کاهش یابد. دولت‌ها ممکن است در پاسخ به این تهدیدات، تلاش کنند اینترنت را به‌عنوان بخشی از هرگونه کارزار اطلاع‌رسانی عمومی در اختیار

کامل خود داشته باشند. بااین‌حال امکان چنین کنترلی بر فضای رسانه‌های جدید وجود ندارد و احتمال بیشتر آن است که دولت‌ها برای شکل‌گیری و تداوم حمایت داخلی از هر اقدامی که با درجه بالایی از ابهام و عدم اطمینان در حوزه جنگ اطلاعاتی مواجه است، با مشکلات جدی روبرو شوند (Molander, Riddile and Wilson, 1996:1).

٤-٢-٤- اطلاعات استراتژیک

واقعیت این است که نقاط ضعف و اهداف استراتژیک جنگ اطلاعاتی جدید به‌خوبی درک نشده‌اند، درنتیجه این امر روش‌های کلاسیک جمع‌آوری و تجزیه‌وتحلیل اطلاعات دیگر کارایی لازم را ندارند؛ بنابراین لازم است یک زمینه تجزیه‌وتحلیل جدید متمرکز بر جنگ اطلاعاتی استراتژیک ایجاد شود. در این راستا باید اشاره کرد روش‌های سنتی جمع‌آوری و تجزیه‌وتحلیل اطلاعات، در مقابله با چالش‌های هوشمند جنگ اطلاعاتی استفاده محدودی دارند. به‌هرحال این‌یک واقعیت است که در دنیای امروزی، شناسایی اهداف، جمع‌آوری و تخصیص منابع اطلاعاتی به دلیل تغییر سریع ماهیت تهدیدات دشوار است و معمولاً آسیب‌پذیری‌ها خیلی دیر شناسایی می‌شوند. به‌طور خلاصه و تحت تأثیر تغییر شرایط جهانی، دولت‌ها ممکن است در شناسایی دشمنان بالقوه و اهداف و توانایی‌های آن‌ها مشکلات جدی داشته باشد. یکی از نتایج این امر این است که روابط سازمانی جدیدی در جامعه اطلاعاتی و بین جامعه اطلاعاتی و نهادهای دیگر موردنیاز است. همچنین ممکن است بازسازی نقش‌ها و مأموریت‌ها مورد نیاز باشد (Molander, Riddile and Wilson, 1996: 1).

٤-٢-٥- مشکل هشدار تاکتیکی و ارزیابی حمله

در حال حاضر در هیچ‌کدام از کشورهای جهان هیچ سیستم هشدار تاکتیکی کافی برای تمایز بین حملات استراتژیک جنگ اطلاعاتی و سایر فعالیت‌های تخریبی فضای سایبری ازجمله جاسوسی سایبری وجود ندارد و این مشکلی است که در هنگام بحران سایبری و در خلال جنگ اطلاعاتی مشکل‌زا خواهد بود. درواقع این ویژگی جنگ اطلاعاتی جدید، مشکلات جدیدی را در فضای سایبری ایجاد می‌کند. یکی از این مشکلات ایجاد تمایز بین حملات و سایر رویدادها مانند تصادفات سایبری، خرابی سیستم یا هک توسط جویندگان هیجان یا کسانی است که به خاطر سرگرمی هک می‌کنند. پیامد اصلی این ویژگی‌ها این است که دولت‌ها ممکن است نداند چه زمانی حمله در جریان است، چه کسی حمله می‌کند یا در نهایت چگونه حمله خواهد کرد (Molander, Riddile and Wilson, 1996: 1).

٤-٢-٦- مشکل در ایجاد و پایداری ائتلاف‌ها

اتکا به ائتلاف‌ها در حوزه اطلاعاتی، احتمالاً آسیب‌پذیری وضعیت‌های امنیتی کشورها در برابر حملات استراتژیک جنگ اطلاعاتی را کاهش می‌دهد و به مزیت استراتژیک نامتناسب

مخالفان ضربه می‌زند. بااین‌حال کمتر کشوری است که در حوزه جنگ اطلاعاتی با اطمینان همکاری و مشارکت کند (Molander, Riddile and Wilson, 1996: 1). به تعبیری دیگر کشورها معمولاً به علت نداشتن اطمینان کامل به همدیگر، در مورد اشتراک اطلاعات به‌شدت حساس و بدبین هستند. در این زمینه حتی کشورهای عضو ناتو و متحدان آمریکا که باهم اشتراک منافع گسترده‌ای دارند، باز در حوزه ایجاد مراکز مشترک اطلاعاتی نگران هستند. به‌هرحال بخشی از این حساسیت و نگرانی به‌دلیل محافظه‌کاری عقلانی است که در سیستم‌های اطلاعاتی وجود دارد.

نتیجه‌گیری

واقعیت این است که امروزه در حوزه نظری و عملی، نوعی سردرگمی در تعریف و تشخیص جنگ‌های نوینی چون جنگ اطلاعاتی، جنگ سایبری، جنگ‌ترکیبی و جنگ ادراکی، شناختی یا معرفتی وجود دارد. به‌واقع همین تنوع گسترده اسامی جنگ‌های نوین، در کنار شباهت‌های مفهومی و مصداقی گسترده‌ای که باهمدیگر دارند، خود گویایی وضعیت بغرنج موجود در تعریف و تشخیص جنگ‌های نوین است. به همین دلیل برخی تلاش می‌کنند از یک تعبیر خاص به‌عنوان‌مثال جنگ‌ترکیبی برای انواع و اقسام جنگ‌های نوین استفاده کنند که این امر چندان با واقعیات موجود و تنوع جنگ‌های نوین ازنظر مفهومی و مصداقی هم‌خوان نیست. بر این اساس می‌توان گفت جهان خواسته یا ناخواسته، تحت تأثیر انقلاب فنّاوری و به‌خصوص انقلاب اطلاعات و ارتباطات و البته از همه مهم‌تر انقلاب سایبری، با امکاناتی مواجه شده است که نتیجه آن شکل‌گیری انواع جدیدی از جنگ‌های نوین و اشکال جدیدی از جنگ‌های کلاسیک است که آمادگی برای مقابله با آن‌ها بسیار مشکل‌آفرین است. البته در تمامی جنگ‌های نوین یک ویژگی کاملاً مشترک وجود دارد که می‌توان آن را کلید فهم مفهومی و مصداقی جنگ‌های نوین و همچنین آمادگی برای برتری در راه مدیریت و مقابله با آن‌ها ارزیابی کرد.

در این راستا ویژگی مشترک تمامی جنگ‌های نوین، نقش برجسته فناوری اعم از فناوری اطلاعاتی، ارتباطی و سایبری و در یک‌کلام علم و دانش است که هم جنگ‌های نوینی چون جنگ سایبری را شکل داده‌اند و هم جنگ‌های نظامی گذشته را در ابعاد مختلف با تغییر شکل و محتوا مواجه نموده‌اند. لازم به اشاره است که تأثیرات بنیادین علم و دانش بر جنگ نظامی و جنگ‌های نوین فراتر از بحث انقلاب در امورات نظامی است و دانش‌های نوین همچون دانش سایبری و به‌ویژه هوش‌مصنوعی در حال تغییر بنیادین مفهوم و محتوای جنگ در عرصه روابط بین‌الملل هستند. بر این اساس راه اصلی آمادگی برای جنگ‌های کلاسیک و نوین، پیشگامی در علم و دانش است. به شکل خاص نیز در مورد جنگ اطلاعاتی همین موضوع صادق است. البته

همان‌گونه که گفته شد، این نوع جنگ قدمتی به درازای تاریخ و هم‌زمان با جنگ‌های نظامی بین اقوام، قبایل، ملل، دولت‌شهرها و کشورها دارد. بااین‌حال تحت تأثیر انقلاب ارتباطات و اطلاعات و انقلاب سایبری، جنگ اطلاعاتی اشکال جدیدی به خود گرفته و از سطح عملیاتی و تاکتیکی به سطح راهبردی راه‌یافته و ابعاد سیاسی، اقتصادی، فرهنگی و اجتماعی و حتی ادراکی و شناختی را هم دربرگرفته است. بر این اساس امروزه جنگ اطلاعاتی در عالی‌ترین سطحش جنگی است برای تغییر ادراک، فهم و دانش دشمن.

References

1. Andrew Mumford (2020), Ambiguity in hybrid warfare, at: Https://www.hybridcoe.fi/wp-content/uploads/2020/09/202009_Strategic-Analysis24-1.pdf
2. Brian, Lewis (2021), Information Warfare, at: https://fas.org/irp/eprint/snyder/infowarfare.htm
3. Brigadier General Gagnon (2020), Information Warfare, Cyberspace Objectives, and the US Air Force, at: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/SLP-Gagnon.pdf
4. Buley, Ben (2014), The New American Way of War Military Culture and the Political Utility of Force, London: Routledge
5. Cunningham, Conor (2020), A Russian Federation Information Warfare Primer, at: https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/#_ftnref5
6. Ciger E. (2021). The greatest security threat in the post-reality era; Why is it becoming increasingly difficult to get accurate information to people? BBC Persian Site. February 23. at: https://www.bbc.com/persian/magazine-56112997
7. Danesh, Farshid and Razieh, Zahedi (2011), Typology of Information Battles and Cyber Wars, *Global Media Journal*, 6(2), Summer and Autumn, 151-166. **(In Persian)**
8. Defense Primer: Information Operations (2020), at: https://fas.org/sgp/crs/natsec/IF10771.pdf.

9. Doagooyan, D. (2020). Soft Warfare of Satellite Television Networks in the Field of International Communications. *International Studies Journal (ISJ)*, 17(2), 115-130. doi: 10.22034/isj.2020.120609**(In Persian)**
10. Ejazi, E., Ghorbani, A., Simbar, R., jansiz, A. (2020). The Impact of US Mainstream Mass Media on American Foreign Policy toward Iran (2007-2020). *International Studies Journal (ISJ)*, 16(4), 23-45. doi: 10.22034/isj.2020.110059**(In Persian)**
11. Information Warfare (2005), at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf
12. Lewis Internet Users, (2021), at: https://www.internetlivestats.com/internet-users/
13. Kalhor, Reza (2000), Information Warfare and its Role in Future Wars, *Scientific Journal of Defense Policy*, 10(32-33), 27-56. **(In Persian)**
14. Kapoor**,** BM (2009), The Art of Perception Management in Information Warfare Today, at: https://usiofindia.org/publication/usi-journal/the-art-of-perception-management-in-information-warfare-today-2/
15. Khan, Nazrul (2015), Perception management; how steers the perception of the public, at: https://www.linkedin.com/pulse/perception-management-how-steers-public-nazrul-khan
16. Kozloski, Robert (2018), Knowing Yourself is key in Cognitive Warfare, at: https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=9931
17. Military intelligence training (2021), at: https://www.groupedci.com/offers/military-intelligence-training/
18. Molander, Roger, Riddile, Andrew and Wilson, Peter (1996), Strategic Information Warfare A New Face of War, at: https://www.rand.org/pubs/monograph_reports/MR661.html
19. Niazi, Ali and Bijan, Moradi (2006), Information & Information Warfare, *Military Science and Tactics (QJMST)*, 3(5), Summer, 183-193. **(In Persian)**
20. Pomerleau, Mark (2020) The new ways the military is fighting against information warfare tactics, at: https://www.c4isrnet.com/information-warfare/2020/07/20/the-new-ways-the-military-is-fighting-against-information-warfare-tactics/aaa
21. Ramlee Sulaiman (2005), information warfare, at: https://www.giac.org/paper/gsec/1870/information-warfare/103284

22. Rolington, Alfred (2013), Strategic Intelligence for the 21st Century: The Mosaic Method. Oxford University Press.
23. Russia's new strategy: information warfare and hybrid warfare (2017), at: mshrgh.ir/699463 **(In Persian)**
24. Sherman, J. Arampatzis, A. & Cobaugh, P, (2018), An Assessment of Information Warfare as a Cybersecurity Issue, at: https://www.realcleardefense.com/articles/2018/06/18/an_assessment_of_information_warfare_as_a_cybersecurity_issue_113541.html
25. Staats, Beth (2021), Misinformation, Disinformation, Malinformation: What's the difference? at: https://www.minitex.umn.edu/news/elibrary-minnesota/2021-02/misinformation-disinformation-malinformation-whats-difference
26. Tanner, Jonathan (2020), 10 things to know about misinformation and disinformation, at: https://www.odi.org/sites/odi.org.uk/files/resource-documents/10_things_to_know_about_misinformation_and_disinformation.pdf
27. Troianovski, A. & Warrick, J. (2018), How a Powerful Russian Propaganda Machine Chips Away at Western Notions of Truth, at: https://www.washingtonpost.com/graphics/2018/world/national-security/russian-propaganda-skripal-salisbury/
28. Torabi, Ghasem, (2015), Cyber revolution in the field of security, *Journal of National Security Studies,* 30(1), 18-29. **(In Persian)**
29. Torabi, Ghasem, (2019), Cyber revolution and change in the nature of power and national security, *Journal of National Security Studies*, 76(1), 45-73. **(In Persian)**
30. What is Propaganda? (2017). Tebyan Site. December 22. At:
https://article.tebyan.net/393675/%D9%BE%D8%B1%D9%88%D9%BE%D8%A7%DA%AF%D8%A7%D9%86%D8%AF%D8%A7-%DA%86%DB%8C%D8%B3%D8%AA- **(In Persian)**