فصلنامه راهبرد سیاسی
سال ششم، شماره ۱، پیاپی ۲۰، بهار ۱۴۰۱
صفحات: ۲۱-۱
تاریخ دریافت: ۱۴۰۰/۱۲/۲۰ ؛ تاریخ پذیرش نهایی: ۱۴۰۱/۰۲/۲۷
نوع مقاله: پژوهشی

تبیین مفهومی و محتوایی جنگ‌های نوین در عرصه روابط بین‌الملل

علیرضا رضایی* / قاسم ترابی**

چکیده

هدف مقاله حاضر تبین مفهومی و محتوایی جنگ‌های نوین ازجمله جنگ سایبری، جنگ شناختی، جنگ اطلاعاتی و جنگ ترکیبی است. در این راستا سؤال اصلی مقاله این است که در مفهوم‌شناسی جنگ‌های نوین، چه عناصر مشترکی وجود دارد؟ در پاسخ به سؤال فوق این فرضیه موردسنجش قرار می‌گیرد که فناوری مهم‌ترین عنصر مشترک در تمامی جنگ‌های نوین محسوب می‌شود. به تعبیری دیگر، درنهایت آنچه باعث شده جنگ‌های نوینی چون جنگ سایبری، جنگ شناختی و جنگ ترکیبی شکل بگیرد و یا باعث تحول جنگ‌های کلاسیک ازجمله جنگ اطلاعاتی به ابعاد جدیدی شده است، بحث انقلاب در عرصه فناوری و به‌ویژه انقلاب سایبری است. در این راستا سطح آمادگی جهت مقابله با چنین جنگ‌هایی، بستگی فراوانی به سطح دانش و فناوری هر کشوری دارد. با توجه به این امر، مقاله حاضر قصد دارد چهار حوزه جدید جنگ شامل حوزه سایبری، شناختی، اطلاعاتی و ترکیبی را موردبحث و بررسی قرار دهد و ضمن واکاوی مفهومی و محتوایی، نقش برجسته فناوری در ابعاد مختلف آن‌ها را مورد توجه قرار دهد. روش مورد استفاده در این مقاله، روش توصیفی و تحلیلی و بر پایه روش کتابخانه‌ای و اینترنتی است.

کلید واژه‌ها

جنگ‌های نوین، جنگ سایبری، جنگ شناختی، جنگ اطلاعاتی و جنگ ترکیبی.

* دانشیار روابط بین الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران (نویسنده مسئول) ir.alirezarezaei@gmail.com
** دانشیار روابط بین الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران

مقدمه

انقلاب در عرصه ارتباطات و اطلاعات و به‌ویژه انقلاب گسترده سایبری باعث تحول در ابعاد اجتماعی، سیاسی، اقتصادی و البته نظامی شده است. درواقع انقلاب فناوری به‌خصوص انقلاب سایبری پدیده جنگ و دفاع را چنان تحت تأثیر قرار داده است که به‌آسانی می‌توان انقلاب سایبری را بزرگ‌ترین و خاص‌ترین نقطه‌عطف در مطالعات امنیتی و راهبردی و در حوزه جنگ و دفاع ارزیابی کرد. در این راستا، انقلاب سایبری در عرصه جنگ و دفاع، باعث شکل‌گیری جنگ‌های نوینی چون جنگ سایبری، جنگ شناختی و جنگ ترکیبی شده است که در آن‌ها از فناوری برای حصول نتیجه و هدف استفاده می‌شود. کشورهایی که در چنین جنگ‌هایی برتری در حوزه علم و فناوری دارند، خیلی راحتر از قبل می‌توانند با حداقل هزینه اهداف راهبردی خود را تأمین کند. همچنین فناوری توانسته به جنگ‌های کلاسیک ابعاد تازه‌ای دهد. به‌عنوان نمونه، تحت تأثیر انقلاب ارتباطات و اطلاعات و به‌ویژه انقلاب سایبری، جنگ اطلاعاتی بین کشورها از حوزه نظامی به حوزه‌های دیگر ازجمله سیاسی، اقتصادی، فرهنگی و اجتماعی و از سطح عملیاتی و تاکتیکی به سطح راهبردی تسری یافته است. بر این اساس اصولاً علم و دانش و فناوری‌های نوین، چنان مفهوم و مصداق جنگ را تغییر داده‌اند که تعبیر جنگ به‌تنهایی نمی‌تواند گویایی همه‌چیز باشد. درواقع به همین دلیل است که بعد از کلمه جنگ پسوند دیگری همچون سایبری، شناختی، اطلاعاتی و ترکیبی می‌آید تا کامل‌کننده معنای جدیدی برای جنگ باشد. با توجه به این مسائل، هدف مقاله حاضر تبیین مفهومی و محتوایی جنگ‌های نوین ازجمله جنگ‌سایبری، جنگ شناختی، جنگ‌اطلاعاتی و جنگ ترکیبی با توجه به انقلاب ارتباطات و اطلاعات و به‌ویژه انقلاب سایبری است. در این راستا سؤال اصلی مقاله این است که در مفهوم‌شناسی جنگ‌های نوین، چه عناصر مشترکی وجود دارد؟ در پاسخ به سؤال فوق این فرضیه موردسنجش قرار می‌گیرد که فناوری مهم‌ترین عنصر مشترک در تمامی جنگ‌های نوین محسوب می‌شود. به تعبیری دیگر، درنهایت آنچه باعث شده است جنگ‌های نوینی چون جنگ سایبری، جنگ شناختی و جنگ ترکیبی شکل بگیرند و یا باعث تحول جنگ‌های کلاسیک ازجمله جنگ اطلاعاتی به ابعاد جدیدی شده است، بحث انقلاب در عرصه فناوری و به‌ویژه انقلاب سایبری است. با توجه به این امر، مقاله حاضر قصد دارد چهار حوزه جدید جنگی شامل حوزه سایبری، شناختی، اطلاعاتی و ترکیبی را موردبحث و بررسی قرار دهد و ضمن واکاوی مفهومی و محتوایی، نقش برجسته فناوری در ابعاد مختلف آن‌ها را موردتوجه قرار دهد.

۱- چارچوب مفهومی

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. 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 ۴۰ درصد 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»[4] 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 از 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. 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

---

1 .Cyber Communication Information Revolution
2 .Cyber Revolution
3 .Global village
4 .The International Telecommunication Union

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 (ترابی، طاهریزاده، ۵۱-۵۰).

ضمن اینکه انقلاب سایبری یک مفهوم گسترده است که دربرگیرنده آخرین تحولات فناوری در شاخههای مختلف علم ازجمله هوش مصنوعی[1]، یادگیری ماشینی[2] و محاسبات کوانتومی[3]، اینترنت رفتار[4] و اینترنت بدن[5] است که هرکدام خود سرمنشأ تغیر و تحولات گسترده و گاه انقلابی در زندگی انسان خواهند شد. بهعنوان نمونه بسیاری از کارشناسان بر این باورند که هوش مصنوعی تمامی ابعاد زندگی فردی و اجتماعی در تمامی ابعاد را چنان تغییر خواهد داد که زندگی پیش و پس از هوش مصنوعی چندان قابل قیاس نخواهند بود .(Gregory, 2021:1) بر این اساس انقلاب سایبری را میتوان تعبیری کلان و جامع برای تحولات انقلابی در تمامی عرصههای علمی مرتبط با فضای سایبر در نظر گرفت که هم ارتباطات انسانها و جوامع را بهشدت گسترده و آسان نموده است و هم تمامی عرصههای سیاسی، اقتصادی، فرهنگی، اجتماعی را دچار تغییر و تحولات بنیادین خواهد کرد.

۲- جنگ سایبری

هیچ تعریف واحدی از جنگ سایبری وجود ندارد. بااینحال با مطالعه و مقایسه تعاریف مختلفی که از جنگ سایبری ارائهشده است، میتوان عناصر مشترکی ازجمله بازیگری دولت، استفاده از فضای سایبر و ایجاد تخریب درنتیجه حمله را شناسایی کرد. بر این اساس در ادامه چندین تعریف که بیشتر مورد پذیریش جامعه علمی و امنیتی هستند ارائه میشود تا هم عناصر مشترک آنها مشخص شوند و هم تحول مفهوم جنگ سایبری موردبحث قرار گیرد. معمولاً جنگ سایبری برای توصیف اقداماتی مورداستفاده قرار میگیرد که زیرساختهای حیاتی را موردحمله قرار میدهند. جنگ سایبری مانند یک حمله مسلحانه است که عمداً باعث اثرات مخربی بهعنوانمثال مرگ و یا صدمه جسمی و یا تخریب اموال میشود. نکته کلیدی اینجاست که فقط دولتها، ارگانهای دولتی یا افراد یا گروههای تحت حمایت دولت میتوانند درگیر جنگ سایبری شوند (Cyberwarfare, 2021:1)؛ بنابراین جنگ سایبری جنگی است که از طریق رایانهها و شبکههای متصل به آنها و توسط دولتها یا پروکسیهای آنها علیه سایر دولتها انجام میشود. جنگ سایبری معمولاً

1. Artificial Intelligence
2. Machine Learning
3. Quantum Computing
4. Interne of Behaviors
5. Internet of Bodies (IoB)

به‌منظور برهم زدن، تخریب یا انکار استفاده از سیستم‌های سایبری علیه شبکه‌های دولتی و نظامی کشور یا کشورهای هدف انجام می‌شود. جنگ سایبری را نباید با استفاده تروریست‌ها از فضای سایبری یا جاسوسی اینترنتی یا جرائم اینترنتی اشتباه گرفت. حتی اگر در هر چهار نوع فوق، خرابکاران از روش‌های مشابهی استفاده کنند، تعریف همه آن‌ها به‌عنوان جنگ سایبری تفسیر صحیحی نیست .(Sheldon, 2021:1)

در تعریفی دیگر از جنگ سایبری چنین آمده است:«جنگ سایبری درگیری رایانه‌ای یا شبکه‌ای است که شامل حملاتی باانگیزه سیاسی توسط یک دولت-ملت علیه یک یا چند دولت-ملت دیگر است. در این نوع حملات، بازیگران وابسته به یک یا چند دولت-ملت تلاش می‌کنند از طریق فضای سایبر فعالیت دولت‌های دیگر خصوصاً برای تأمین اهداف استراتژیک یا نظامی را مختل کنند. اگرچه جنگ سایبری به‌طورکلی به حملات سایبری انجام‌شده توسط یک دولت ملی علیه کشور دیگر اشاره دارد، اما همچنین می‌تواند حملات گروه‌های تروریستی یا گروه‌های هکر نیابتی باهدف پیشبرد اهداف دول خاص را نیز توصیف کند»(Rosencrance, 2019:1). جنگ سایبری می‌تواند اشکال مختلفی داشته باشد، ازجمله:

- ویروس‌ها، کرم‌های رایانه‌ای و بدافزارهایی که می‌توانند زیرساخت‌های مهم و سیستم‌های نظامی را هدف قرار دهند.
- حملات انکار سرویس[1]، وقایع امنیتی سایبری هستند که مانع دسترسی کاربران به سیستم‌های رایانه‌ای، دستگاه‌ها یا سایر منابع شبکه می‌شوند.
- هک و سرقت داده‌های مهم از وزارتخانه‌ها، مراکز، مؤسسات و مشاغل دولتی از طریق باج‌افزار که سیستم‌های رایانه‌ای را گروگان می‌گیرد تا زمانی که قربانیان باج بدهند .(Rosencrance, 2019:1)

در تعریفی دیگر جنگ سایبری شامل اقداماتی توسط یک دولت-ملت برای حمله و تلاش برای آسیب رساندن به رایانه‌ها یا شبکه‌های اطلاعاتی کشور دیگری از طریق ویروس‌های رایانه‌ای یا حملات انکار سرویس است(Cyber Warfare, 2021:1) . رنجر[2] در تعریفی مشابه اما کامل‌تر، جنگ سایبری را این‌گونه تعریف می‌کند: « جنگ سایبری به استفاده از حملات دیجیتالی مانند ویروس‌های رایانه‌ای و هک کردن توسط یک کشور برای ایجاد اختلال در سیستم‌های رایانه‌ای حیاتی کشور دیگر، باهدف ایجاد آسیب، مرگ و نابودی اشاره دارد. به باور وی در جنگ‌های آینده، هکرها با استفاده از کد رایانه‌ای برای حمله به زیرساخت‌های دشمن، در کنار سایر نیروهای نظامی می‌جنگند (Ranger, 2018:1). فعالیت‌های خصمانه در فضای سایبری را

1. Denial-of-Service Attacks (DoS)
2. Ranger

می‌توان با توجه به انواع فعالیت‌های انجام‌شده و آسیب‌های ناشی از آن درجه‌بندی کرد. آنچه در زیر می‌آید یک طبقه‌بندی است که توسط تابانسکی[1] به ترتیب شدت نزولی مرتب‌شده است:

۱. حمله به اهداف غیرنظامی که باعث صدمه فیزیکی می‌شود؛

۲. به هم ریختن و تخریب زیرساخت‌های مهم اطلاعات ملی؛

۳. اخلال در اهداف نظامی در قلمرو حاکمیت دولت‌ها؛

۴. اخلال در اهداف نظامی در خارج از قلمرو حاکمیت دولت‌ها؛

۵. فعالیت جنایی و جاسوسی صنعتی؛

۶. جمع‌آوری اطلاعات، جستجوی موارد رایج آسیب‌پذیری‌های امنیتی و آزمودن‌های نفوذ؛

۷. مدیریت یک کارزار تبلیغاتی رسانه‌ای خرابکارانه، سوءاستفاده و تحریف کردن وب‌سایت‌های رسمی (Tabansky, 2011:82-83).

از موارد فوق تنها مورد یک تا پنج است که مشمول تعریف جنگ سایبری می‌شود، چراکه مسئله تخریب جزو عناصر اصلی تشکیل‌دهنده جنگ سایبری است. ضمن اینکه به‌منظور تعیین اینکه حمله سایبری بخشی از یک جنگ سایبری باشد، چندین ویژگی دیگر باید بررسی شود:

۱. منبع و منشأ حمله: اینکه یک کشور پشت حمله قرار دارد یا بازیگران دیگر؟ اگر عامل حمله و تخریب کشوری خاص باشد، مشمول جنگ سایبری است، در غیر این صورت نمی‌توان حمله را جنگ سایبری نامید.

۲. آیا حمله می‌توانست خسارتی ایجاد کند و یا اینکه واقعاً باعث خسارت و تلفات شده است؟ اگر حمله سایبری هدایت‌شده توسط دولت یا عاملان آن خسارت ایجاد کند یا باهدف ایجاد خسارت طراحی‌شده باشد، حمله را می‌توان جنگ سایبری ارزیابی کرد، در غیر این صورت ممکن است مشمول تعریفی دیگری همچون جاسوسی سایبری شود.

۳. آیا حمله به برنامه‌ریزی پیچیده‌ای نیاز داشته و منابع هماهنگ شده‌ای که عمدتاً در اختیار دولت‌ها قرار دارد در آن استفاده‌شده است؟(Tabansky, 2011:82-83). البته با توجه به ویژگی‌های فضای سایبری امروز، پاسخ به این سؤالات بسیار دشوار است، بااین‌حال اگر جواب این سؤالات کاملاً روشن نشود، نمی‌توان حمله سایبری را جنگ سایبری نامید.

نکته مهم دیگر در مورد جنگ سایبری حدت و شدت آن است. در بسیاری از موارد، سیستم‌های رایانه‌ای هدف نهایی نیستند، بلکه به دلیل نقشی که در مدیریت زیرساخت‌های دنیای واقعی مانند فرودگاه‌ها یا شبکه‌های برق دارند هدف قرار می‌گیرند. در یک جنگ سایبری ممکن است هدف محدود باشد، مثلاً حمله

1. Tabansky

سایبری به شبکه برق یا نیروگاه‌های هسته‌ای صورت گیرد، اما ممکن است جنگ سایبری همه‌جانبه و گسترده باشد و اهداف گسترده‌ای را دربرگیرد .(Ranger, 2018:1)

۳- جنگ شناختی

در ساده‌ترین تعریف امنیت شناختی[1] به معنای محافظت از دانش، فهم و آگاهی شهروندان است (Seger, Avin, and others, 2020:23-50). به تعبیر سیگر امنیت شناختی شامل کسب اطمینان از آگاهی واقعی نسبت به چیزهایی است که جامعه فکر می‌کند درست هستند. همچنین وجه دیگر امنیت شناختی شامل توان تشخیص ادعاهای غلط و بی‌مدرک و ایجاد سامانه‌های اطلاعاتی مقاوم در برابر تهدیدهای شناختی مانند اخبار جعلی[2] می‌شود. لازم به اشاره است، معرفت یا اپیستیم[3] یک اصطلاح فلسفی یونانی به معنای دانستن است؛ بنابراین امنیت شناختی شامل اطمینان از این می‌شود که شهروندان یک کشور بدانند که چه چیزی را می‌دانند و اینکه بتوانند ادعاهای بی‌اساس یا نادرست را تشخیص دهند و اطمینان یابند که اکوسیستم‌های اطلاعاتی[4] نسبت به تهدیدهای شناختی مانند اخبار جعلی مقاوم هستند (سیگر،۱۳۹۹:۱). بنا به تحقیقات صورت‌گرفته توسط یک گروه تحقیقاتی به رهبری الیزابت سیگر[5]، در عصر حاضر چهار روند مختلف امنیت شناختی را تهدید می‌کنند که آن‌ها را می‌توان شگردهای جنگ شناختی نامید. اول مسئله اطلاعات گسترده و کمبود توجه[6] است. در این راستا، در شرایطی که اینترنت حجم گسترده‌ای از اطلاعاتی تاییدنشده را در دسترس همگان قرار می‌دهد، تشخیص درست از نادرست کار سختی است. اطلاعات هنگفت و کمبود توجه به این معنی است که دولت‌ها، خبرنگاران، نمایندگان منافع مختلف و دیگران باید با یکدیگر بر سر ایجاد ذهنیت در بین مخاطبان رقابت کنند و دراین‌بین کسی برنده می‌شود که معمولاً روش بهتری دارد و نه لزوماً کسی که واقعیت را می‌گوید. مسئله دوم حباب‌های تصفیه‌کننده[7] و عقلانیت محدود[8] است. درواقع یکی از پیامدهای نگران‌کننده مسئله کمبود توجه در فضای اطلاعات گسترده، ایجاد حباب‌های تصفیه‌کننده است. حباب‌های تصفیه‌کننده روندهای هستند که باعث می‌شوند افراد فقط با عقاید فعلی خود برخورد داشته باشند و نظرات مخالف را نبینند. افراد معمولاً در برخورد با اطلاعات بیش‌ازحد گسترده، به‌طور طبیعی بیشتر به

1. Epistemic Security
2. Fake News
3. Episteme
4. Information Ecosystem
5. Elizabeth Seger
6. Attention Scarcity
7. Filter Bubbles
8. Bounded Rationality

کسانی که شبیه خودشان هستند توجه می‌کنند و کمتر سراغ چهره‌های ناشناخته می‌روند. پیامد شناختی این حباب‌های تصفیه‌کننده، به امری منتهی می‌شود که به عقلانیت محدود معروف است. لازم به اشاره است که دسترسی به اطلاعات، پایه و اساس استدلال و تصمیم‌گیری خوب است، لذا محدود کردن اطلاعات ورودی با سنگر گرفتن در این حباب‌ها، توان استدلال خوب را کاهش می‌دهد. مسئله سوم سوءاستفاده دشمن از جریان اطلاعات[1] است. در عصر انقلاب سایبری، پخش و دسترسی به اطلاعات از هرزمانی راحت‌تر شده است؛ اما جنبه منفی این تحول این است که می‌توان از همان فناوری‌ها برای انتشار اتفاقی یا عمدی اطلاعات غلط یا گمراه‌کننده استفاده کرد. معمولاً بازیگران مختلفی مانند افراد، سازمان‌ها، یا حکومت‌ها، عمداً اطلاعات را دست‌کاری می‌کنند تا دریافت‌کنندگان را گمراه کنند و عقاید غلط را ترویج دهند (سیگر، ۱:۱۳۹۹).

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 اغلب مبتنی بر الگوهای رفتاری و فیلم‌های کوتاه هستند که به‌طور گسترده در برنامه‌های پیام بسته[2] مانند فیس‌بوک و واتساپ به اشتراک گذاشته می‌شود. عاملان اطلاعات نادرست می‌توانند وب‌سایت‌ها و یا حساب‌های جعلی در رسانه‌های اجتماعی[3] ایجاد کنند تا پیام‌های خود را میزبانی کنند، این تاکتیکی معروف است که به آن تبلیغ محاسباتی[4] می‌گویند. ضمن اینکه این ربات‌ها خودکار هستند، اما می‌توانند برای جلب‌توجه، حساب‌های جعلی ایجاد کرد. همچنین افراد می‌توانند خود را در گروه‌های موجود فیس‌بوک یا واتساپ عضو کنند و از اخبار جعلی برای انتشار دروغ در میان حساب‌های قانونی استفاده کنند، سپس 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 هوش مصنوعی برای ایجاد روش‌های پیچیده‌تر برای انجام این کار استفاده می‌کنند، ازجمله ایجاد حساب‌های ربات واقع‌گرایانه‌تر و فیلم‌های جعلی که برخی محققان ازجمله تانر[5] قبلاً آن را جدی‌ترین تهدید نامیده‌اند .(Tanner,2020:1-13)

در این زمینه و برای روشن شدن بحث می‌توان به نتایج تحقیقی که چندی پیش ژورنال ساینس منتشر کرد اشاره کرد. این پژوهش با تحلیل میلیون‌ها توییت مربوط به سال‌های ۲۰۰۶ تا ۲۰۱۷ نتایج نشان داد: «در

1. Action by Adversaries and Blunderers
2. Closed Messaging Apps
3. .Fake Social Media Accounts
4. Computational Propaganda
5. Jonathan Tanner

تمامی حوزه‌های زندگی اجتماعی، اطلاعات و اکاذیب بسیار دامنه‌دارتر، سریع‌تر، عمیق‌تر و گسترده‌تر از حقایق نشر می‌یابد». این پژوهش همچنین دریافت که «تأثیر اخبار سیاسی جعلی به‌مراتب پررنگ‌تر از اخبار جعلی مربوط به تروریسم، بلایای طبیعی، علم، افسانه‌های محلی یا اطلاعات مالی است». این تحلیل عظیم با جمع‌آوری داده‌ها، به این ذهنیت متداول می‌پردازد که رسانه‌های اجتماعی به‌عنوان پلتفرمی برای نشر اخبار، گرایش به خبرهای تائید نشده، احساسی و جعلی دارند و این امر نگران‌کننده است، چون رسانه‌های اجتماعی به نیرویی غالب برای نشر اخبار تبدیل شده‌اند. درمجموع، یافته‌های این تحلیل نشان می‌دهد که «حقیقت شش برابر بیشتر از دروغ طول می‌کشد تا به دست ۱۵۰۰ نفر برسد»(رزنیک،۱۳۹۷:۱).

درنهایت تهدید آخر فرسایش اعتماد[1] است. انسان‌ها به‌طور طبیعی می‌توانند تصمیم بگیرند که به چه کسی اعتماد کنند و به چه کسی اعتماد نکنند. برای مثال، هر چه تعداد کسانی که گفته‌های یک شخص را باور دارند بیشتر باشد، احتمال اعتماد سایر افراد به او بیشتر می‌شود. همچنین از منظر روانشناسی احتمال اعتماد انسان به عضوی از اجتماع خودش بیشتر از افراد خارج از اجتماع است، چراکه منافع و ارزش‌های مشابهی بین آن‌ها وجود دارد. البته افراد از زبان بدن، لحن بیان و سبک سخنرانی برای سنجش صداقت استفاده می‌کنند؛ اما می‌توان بینش و واقعیت‌های فوق را با برخی از فناوری‌های مدرن به خطا انداخت. برای مثال، حباب‌های تصفیه‌کننده می‌توانند عقاید اقلیت را بیشتر در معرض دید قرار دهند و کاری کنند که عقاید اکثریت به نظر برسند. شکی نیست که برخی دیدگاه‌های اقلیت باید در معرض دید قرار بگیرند، اما عادی‌سازی و محترم جلوه دادن روایت‌های افراطی کاری مشکل‌آفرین است. همچنین می‌توان از فناوری برای گمراه کردن بینش‌های ناخودآگاه استفاده کرد. برای مثال، ویدیوهای جعل عمیق[2] به‌گونه‌ای ساخته می‌شوند که در آن‌ها معمولاً نشانه‌ای برای شک وجود ندارد. درنهایت چهار مسئله یا مشکل فوق به حباب شناختی منتهی می‌شوند که یکی از بدترین اتفاقاتی است که ممکن رخ دهد. در جهان حباب‌های شناختی، توانایی عموم مردم برای تشخیص حقیقت از دروغ کاملاً از بین می‌رود. اطلاعات به‌راحتی در دسترس است، اما مردم نمی‌توانند بفهمند چیزی که می‌بینند، می‌خوانند یا می‌شنوند قابل‌اتکا است یا خیر؟. به‌هرحال نتیجه روندهای فوق این است که یک جامعه درنهایت دچار تحول در دانش و بینش می‌شود و مسائل را آن‌گونه که دشمن می‌خواهد می‌بیند، تجزیه‌وتحلیل می‌کند و سپس اقدام می‌کند (سیگر،۱۳۹۹:۱).

از حیث هدف‌شناسی، جنگ شناختی می‌تواند اهداف مختلفی را دنبال کند. معمولاً اولین هدف اساسی جنگ‌شناختی، ایجاد بی‌ثباتی در جمعیت هدف است .بی‌ثباتی به معنای برهم زدن انسجام و وحدت جمعیت

1. Fabrication and Erosion of Trust
2. Deepfake

و مردم هدف است که این امر منجر به بین رفتن همکاری بین آن‌ها می‌شود .در این راستا، کشور مهاجم از طریق جنگ‌شناختی و طرح ایده‌های جدید، اختلافات و قطب‌بندی در جامعه هدف را افزایش می‌دهد .ضمن اینکه در یک جنگ‌شناختی، رهبران بهترین هدف قطبی‌سازی هستند، زیرا جامعه را می‌توان بر اساس حمایت یا مخالفت از آن‌ها دوقطبی کرد .کشور مهاجم می‌تواند جمعیت را به شکل تصادفی هدف قرار دهد و یا در مواردی تنها بر گروهی خاص مثل نظامیان یا اقلیت‌های قومی و زبانی یا گروهای دیگر تمرکز کند. این کار معمولاً از طریق اخبار جعلی، عقاید تفرقه‌انگیز و روایت‌های دروغین انجام می‌شود .تاکتیک‌های جنگ‌شناختی شامل مواردی همچون افزایش قطب‌بندی و ایجاد تفرقه، دوباره زنده کردن جنبش‌های فراموش‌شده، مشروعیت‌زدایی از دولت و رهبران، جدا کردن افراد و گروه‌ها با تأکید و بزرگنمایی اختلافات و تفاوت‌ها، مختل کردن فعالیت‌های کلیدی اقتصادی و برهم زدن زیرساخت‌ها می‌شوند؛ بنابراین هدف اول جنگ‌شناختی بی‌ثبات‌سازی جامعه و کشور هدف و کنار زدن آن از مسیر صحیح افزایش قدرت ملی است. دومین هدف اساسی جنگ‌شناختی، تأثیرگذاری بر جمعیت هدف در مورد موضوعاتی خاص مثل انتخابات یا سیاست خارجی در قبال موضوعی مشخص است. این هدف از طریق نفوذ و دست‌کاری در تفسیر و درک مردم از مسائل مختلف انجام می‌شود. در این راستا، مهاجمان می‌توانند افراد، گروه یا شهروندان را به‌گونه‌ای هدایت کنند که به نفع آن‌ها عمل کنند. لازم به اشاره است که هدف تأثیرگذاری با هدف بی‌ثبات‌سازی متفاوت است، زیرا هدف تأثیرگذاری شکل دادن به ذهنیت هدف اما هدف بی‌ثبات‌سازی ایجاد شورش و بلوا در جامعه است. یکی از نمونه‌های تأثیرگذاری بر شهروندان از طریق جنگ‌شناختی، تأثیرگذاری روسیه بر نتایج انتخابات کشورهای غربی ازجمله انتخابات سال ۲۰۱۶ ایالات‌متحده آمریکا است که نتیجه آن پیروزی غیرمنتظره دونالد ترامپ بود.(Bernal and others, 2020:11-20)

لازم به اشاره است در جهان سایبری امروز، یکی از کارآمدترین ابزارهای جنگ شناختی، شبکه‌های اجتماعی هستند. در همین زمینه ناتو در همکاری با دانشگاه جان هاپکینز[1] و امپریال کالج لندن[2] تحقیقی گسترده در مورد نقش برجسته شبکه‌های اجتماعی در جنگ شناختی انجام داده است. در بخشی از این گزارش آمده است: «توانایی‌های شناختی ما ممکن است توسط رسانه‌های اجتماعی و دستگاه‌های هوشمند تضعیف شود. استفاده از شبکه‌های اجتماعی می‌تواند تعصبات شناختی[3] و خطاهای ذاتی تصمیم‌گیری[4] را

1. Johns Hopkins University
2. Imperial College London
3. Cognitive Biases
4. Innate Decision Errors

افزایش دهد. در کتاب «فکر کردن، سریع و آهسته»[1]، دانیل کانمن[2]، برنده جایزه نوبل به‌خوبی درباره تعصبات شناختی و خطاهای ذاتی تصمیم‌گیری بحث شده است. در این زمینه، کانمن اشاره می‌کند که فیدهای خبری و موتورهای جستجوگر نتایجی را ارائه می‌دهند که با ترجیحات ما مطابقت بیشتری دارند. ما معمولاً اطلاعات جدید را به‌گونه‌ای تفسیر و تأیید می‌کنیم که با باورهای پیش‌فرض ما مطابقت داشته باشند. بر این اساس برنامه‌های پیام‌رسان اجتماعی به‌سرعت کاربران را با اطلاعات جدید به‌روز می‌کنند و باعث ایجاد تعصب در بین آن‌ها می‌شوند، به‌این‌ترتیب افراد اهمیت رویدادهای اخیر را نسبت به گذشته بیش‌ازحد درک می‌کنیم. ضمن اینکه سایت‌های شبکه‌های اجتماعی به شکلی هستند که تائید اجتماعی[3] را القا می‌کنند. افراد در تائید اجتماعی اقدامات و اعتقادات دیگران را با گروه‌های اجتماعی خود مطابقت می‌دهند که این امر تبدیل به اتاق‌های پژواک و تفکر گروهی می‌شود. مشکل دیگر در این زمینه سرعت‌بالای انتشار اخبار و بازنشر و پاسخ به آن‌ها است. در این راستا، سرعت سریع ارسال پیام و انتشار اخبار و احساس نیاز سریع به واکنش در برابر آن‌ها، سریع فکر کردن انعکاسی و احساسی[4] را تشویق می‌کند که در مقابل آرام و منطقی فکر کردن است. اکنون حتی خبرگزاری‌های معتبر نیز از عناوین احساسی برای تشویق انتشار سریع مقاله‌های خبری خود استفاده می‌کنند. درنهایت مشکل آخر نداشتن دقت و کم‌گذاشتن زمان برای خواندن و نشر اخبار است. واقعیت این است که افراد وقت کمتری را به خواندن مطالب اختصاص می‌دهند، حتی اگر دفعات اشتراک آن‌ها را افزایش دهند. همچنین سیستم‌های پیام‌رسان‌های اجتماعی برای توزیع قطعه‌های کوتاه بهینه‌سازی شده‌اند که غالباً از زمینه‌ها و تفاوت‌های مهم چشم‌پوشی می‌کنند. این امر می‌تواند تسهیل و گسترش عمدی و غیرعمدی سوءتفسیر از اطلاعات[5] و روایت‌های وارونه[6] را تسهیل کند. در این راستا اختصار پست‌های شبکه‌های اجتماعی، در ترکیب با تصاویر دیدنی چشمگیر، ممکن است خوانندگان را از درک انگیزه‌ها و ارزش‌های دیگران باز دارد» (Johns Hopkins University & Imperial College London, 2021:1-5).

در جنبه دفاعی، دولت‌ها باید حداقل از اینکه یک جنگ‌شناختی در حال انجام است آگاه باشند. راه‌حل‌های فناوری می‌توانند ابزارهایی را برای پاسخ به برخی از سؤالات اصلی در این زمینه فراهم کنند: آیا کمپینی در جریان است؟ از کجا نشئت‌گرفته است؟ چه کسی آن را اداره می‌کند؟ اهداف مهاجمان چه

1. Thinking, Fast and Slow
2. Daniel Kahneman
3. Social Proofing
4. Reflexively and Emotionally Thinking Fast
5. Intentionally and Unintentionally Misinterpreted Information
6. Slanted Narratives

می‌تواند باشد؟ تحقیقات ناتو نشان می‌دهد که چنین الگوهای تکرارشونده‌ای وجود دارد که می‌توان آن‌ها را طبقه‌بندی کرد. آن‌ها حتی ممکن است امضاهایی منحصر به بازیگران خاص را ارائه دهند که می‌تواند به شناسایی عاملان حمله کمک کند. یک‌راه حل ویژه در این زمینه، استفاده از سیستم نظارت و هشدار جنگ‌شناختی[1] است. چنین سیستمی می‌تواند به شناسایی، وقوع و پیگیری جنگ‌شناختی کمک کند. این امر می‌تواند شامل داشبوردی شود که داده‌های طیف گسترده‌ای از رسانه‌های اجتماعی، رسانه‌های خبری، پیام‌های اجتماعی و سایت‌های شبکه‌های اجتماعی را تلفیق کند. یک داشبورد می‌تواند با شناسایی مکان‌های جغرافیایی و مجازی که از آن پست‌ها، پیام‌ها و اخبار رسانه‌های اجتماعی نشئت می‌گیرد و همچنین از طریق موضوعات موردبحث، احساسات و شناسه‌های زبانی و سایر عوامل، ارتباطات و الگوهای تکراری را آشکار کند. ضمن اینکه استفاده از یادگیری ماشین و الگوریتم‌های تشخیص الگو[2] می‌تواند به‌سرعت در شناسایی و طبقه‌بندی مبارزات نوظهور بدون نیاز به مداخله انسان کمک کند. چنین سیستمی امکان نظارت بی‌درنگ را فراهم می‌کند و هشدارهای به‌موقع را به تصمیم‌گیرندگان ارائه می‌دهد و به آن‌ها کمک می‌کند تا در هنگام ظهور و تکامل جنگ‌شناختی، پاسخ‌های مناسب را تنظیم و آماده کنند (Johns Hopkins University & Imperial College London, 2021:1-5).

۴- جنگ اطلاعاتی

از منظر معنایی، جنگ اطلاعاتی به مفهوم کشمکش بر سر فرایند اطلاعات و ارتباطات است، جنگی که با اعمال نیروی تخریبی در مقیاس وسیع علیه دارایی‌ها و سیستم‌های اطلاعاتی، در برابر رایانه‌ها و شبکه‌هایی که از زیرساخت‌های مهم پشتیبانی می‌کنند، با طرح و برنامه اعمال می‌شود (Brian, 2021:1). ناتو جنگ اطلاعاتی را این‌گونه تعریف می‌کند:«جنگ اطلاعاتی عملیاتی است که به‌منظور کسب برتری اطلاعاتی نسبت به حریف انجام می‌شود. این جنگ شامل کنترل فضای اطلاعاتی، محافظت از دسترسی به اطلاعات شخصی خود، درعین‌حال تلاش در جهت به دست آوردن و استفاده از اطلاعات، تخریب دستگاه‌های اطلاعاتی و ایجاد اختلال در جریان اطلاعات دشمن می‌شود. جنگ اطلاعاتی پدیده جدیدی نیست، اما شامل عناصر ابتکاری درنتیجه توسعه فناوری است که منجر به انتشار سریع‌تر و در مقیاس بزرگ‌تر اطلاعات می‌شوند (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

1. Cognitive Warfare Monitoring and Alert System
2. Machine Learning and Pattern Recognition Algorithms

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 می‌کنید». وزارت دفاع آمریکا در تعریف تکمیلی تأکید می‌کند که جنگ اطلاعاتی «توانایی جمع‌آوری، پردازش و انتشار جریان بی‌وقفه اطلاعات برای دستیابی یا ارتقا اهداف بر روی یک دشمن خاص است، درحالی‌که دسترسی به این توانایی‌ها برای دشمن انکار می‌شود (Ramlee,2005: 1-2). به تعبیری دیگر، جنگ اطلاعاتی جنگ همه‌چیز مرتبط با فریب دشمن است. این جنگ شامل خود 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 دریایی آمریکا جنگ اطلاعاتی را این‌گونه تعریف می‌کند:«جنگ اطلاعاتی غالباً یک اصطلاح موردبحث است و درواقع فاقد تعریف مشترک مورد تائید است؛ اما برای نیروی هوایی آمریکا، جنگ اطلاعاتی به‌عنوان فعالیت‌هایی است که عناصر اطلاعاتی، نظارتی و شناسایی، عملیات فضای مجازی، جنگ الکترومغناطیسی و عملیات را برای دستیابی به نتایج در دو زمان جنگ و صلح اطلاعاتی هماهنگ می‌کند. امروز نیروی هوایی جنگ اطلاعاتی را استفاده از توانایی‌ها و ظرفیت‌های نظامی در محیط اطلاعاتی جهت تأثیر عمدی بر رفتار نیروها و سیستم اطلاعاتی دشمن توصیف می‌کند .(Gagnon, 2020:5) ژنرال تیموتی هوگ[1]، فرمانده جنگ اطلاعات نیروی هوایی آمریکا[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، 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 رشته‌هایی است که به جمع‌آوری، تجزیه‌وتحلیل و انتشار اطلاعات برای واحدهای نظامی و تصمیم‌گیرندگان اختصاص داده می‌شود. اطلاعات نظامی به اطلاعات انسانی[3] و اطلاعات فنی که خود شامل اطلاعات تصویر[4] و اطلاعات الکترونیک[1]

1. Gen. Timothy Haugh
2. Information Warfare Organization
3. Human Intelligence
4. Technical Intelligence – Mainly Imagery Intelligence

است تقسیم می‌شود. فعالیت‌های اطلاعاتی چه در زمان صلح و چه در زمان جنگ در همه سطوح تاکتیکی، عملیاتی و استراتژیک انجام می‌شود .(Military intelligence training, 2021) در تعریفی دیگر گفته‌شده است، اطلاعات نظامی یک‌رشته نظامی است که با استفاده از روش‌های جمع‌آوری و تجزیه‌وتحلیل اطلاعات، به فرماندهان در تصمیم‌گیری‌ها کمک می‌کند. این هدف با ارائه ارزیابی داده‌ها از طیف وسیعی از منابع، به سمت نیازهای مأموریت فرماندهان یا پاسخ به سؤالات به‌عنوان بخشی از برنامه‌ریزی عملیاتی محقق می‌شود. معمولاً برای ارائه تجزیه‌وتحلیل ابتدا نیازهای اطلاعاتی فرمانده مشخص می‌شود، سپس جمع‌آوری، تجزیه‌وتحلیل و انتشار اطلاعات در اولویت قرار می‌گیرد. مناطق موردمطالعه ممکن است شامل محیط عملیاتی، نیروهای متخاصم، دوست و بی‌طرف، جمعیت غیرنظامی در منطقه‌ای از عملیات جنگی و سایر مناطق موردعلاقه شود. فعالیت‌های اطلاعاتی در همه سطوح، از تاکتیکی تا استراتژیک، در زمان صلح و دوره انتقال به جنگ و در طول دوره جنگ انجام می‌شود. اطلاعات استراتژیک به موضوعات گسترده‌ای مانند اقتصاد، تحلیل سیاسی، توانایی‌های نظامی و اهداف دول خارجی و به‌طور فزاینده‌ای بازیگران غیردولتی همچون تروریست‌ها مربوط می‌شود. چنین اطلاعاتی ممکن است علمی، فنی، تاکتیکی، دیپلماتیک یا جامعه‌شناختی باشند. 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 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 مهاجم تصمیم‌گیری کند» ,Blagovest)

---

1. Electronic Intelligence

.(2019:129-133 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 مختلف 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 هر منطقه از جهان را با رویکردی متفاوت و 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 و فهم جمعیت هدف تأثیر می‌گذارد، به‌گونه‌ای که منافع روسیه را تأمین کند. البته برخلاف عملیات سایبری، عملیات اطلاعاتی بسیار قدیمی است که کرملین مدت‌هاست برای تحقق اهداف خود از آن استفاده می‌کند. در این راستا 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، ترول‌ها[1] و ربات‌ها 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

---

1. Internet Trolls

ترول‌ها افرادی هستند که در اتاق‌های گفتگو، تالارها، وب‌نوشت‌ها یا تارنماهای کاربر-محور، پیام‌هایی ارسال می‌کنند که حاوی مطالب ناراحت‌کننده یا جنجال‌برانگیز است.

گسترش داده است. همان‌گونه که گفته شد، 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 جنگ ترکیبی است که اجرای هم‌زمان آن‌ها، باعث هم‌افزایی قدرت کشور مهاجم و آسیب‌پذیری بیشتر کشور مدافع می‌شود .(Mumford, 2020:3)

۵- جنگ ترکیبی

جنگ ترکیبی ابتدا به‌عنوان یک مفهوم توسط فرانک هافمن[1] در سال ۲۰۰۷ توسعه داده شد (Green, 2020:2). به باور هافمن جنگ ترکیبی 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 طریق استفاده از همه ابزارهای سیاسی، نظامی، اقتصادی، اجتماعی، اطلاعاتی، سایبری و زیرساختی را از بین میبرد. جنگ ترکیبی هم چندوجهی است و هم در یک‌زمان در سطوح چندگانه به کار گرفته میشود. این نوع جنگ 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 جنگ ترکیبی فضاهای فیزیکی سنتی مانند زمین، دریا، هوا و فضا بهنحو فزایندهای با فضاهای اجتماعی و برساخته مانند فضای سیاسی، اقتصادی، فرهنگی، اطلاعاتی و سایبری و از همه مهم‌تر فضاهای شناختی و روانی پیوند می‌خورند؛ درنتیجه ضرورت کاربست نیروی 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، بینالمللی و قلمرو عملیاتی و سیاستمداران قرار می‌گیرد و دشمن را وادار به تسلیم یا دادن امتیاز می‌کند .(Mumford, 2020:3) در این بین فن‌آوری‌های نوین و به‌ویژه فناوری‌های سایبری نقش مهمی در جنگ ترکیبی دارند. درواقع فناوری‌های نوین و به‌ویژه هوش مصنوعی راهی برای دستیابی به اهداف سیاسی در منطقه خاکستری در حدفاصل جنگ و صلح فراهم می‌کنند. در بعد دفاعی نیز تحولات جدید فناوری ممکن است گزینه‌هایی را برای شناسایی بهتر، درک عمیق‌تر و دفاع کارامدتر در مقابل حملات ترکیبی ارائه دهد. ازاین‌رو، برای رهبران سیاسی و نظامی و تصمیم‌گیرندگان مهم است که درک کاملی از پیامدهای فن‌آوری‌های جدید در حوزه جنگ ترکیبی داشته باشند .(Thiele,2020:6)

[1]. Frank Hoffman

بر این اساس اصطلاح جنگ ترکیبی برای مشخص کردن زیرمجموعه‌ای ویژه از اقدامات به کار می‌رود که شامل کاربرد استراتژیک استفاده از نیروی ابهام[1] جهت دستیابی به قلمرو یا به دست آوردن اهداف استراتژیک دیگری است. جنگ ترکیبی برخلاف سایر انواع اقدامات ترکیبی مانند اقدامات عملیات دخالت و نفوذ[2] تشکیل‌دهنده فعالیت‌های قابل‌رؤیت اجبارآمیز است. در این راستا، بازیگران جنگ ترکیبی نیازی به انکار کردن اقدامات خود ندارند، چراکه مسئله مسئولیت استفاده از زور جدا از مسئله ابهام است. در این راستا، نکته بسیار مهم و کلیدی این است که هدف از ابهام ضرورتاً پنهان کردن بازیگر واقعی پشت فعالیت‌ها نیست، بلکه نهایتاً ممانعت از یک جواب مشروع و فرار از مسئولیت است. برای مثال می‌توان به جنگ کریمه به‌عنوان مصداق یک جنگ ترکیبی موفق در حوزه ابهام برای رفع مسئولیت اشاره کرد. در جنگ کریمه علی‌رغم اینکه کشورهای غربی می‌دانستند روسیه عامل اصلی بحران و جنگ کریمه است، اما دخالت چنان مبهم و در زیر آستانه تحمل کشورهای غربی بود که روسیه توانست تا حد زیادی از زیر مسؤولیت و عواقب آن فرار کند. به تعبیری دیگر روسیه در جنگ کریمه دقیقاً زیر آستانه تلافی مشروع[3] عمل کرد .(Mumford, 2020:3)

لازم به اشاره است که مفهوم ابهام در مطالعات استراتژی غربی به‌طور تاریخی در ادبیات استراتژی هسته‌ای[4] واقع‌شده است، جایی که با ایده بازدارندگی مرتبط شده است. جان بایلیز[5] در مطالعه استراتژی هسته‌ای بریتانیا[6]، دو مکتب فکری راجع به این مسئله معرفی کرد. او بین استراتژیست‌هایی که از ابهام عمدی[7] در حوزه امکان استفاده از تسلیحات هسته‌ای طرفداری می‌کنند و آن‌هایی که از ابهام ناخواسته[8] طرفداری می‌کنند تمایز قائل شد. جنگ ترکیبی، به‌طور محکم بر پایه آنچه بایلیز آن را ابهام حساب‌شده می‌خواند قرار دارد.(Mumford, 2020:3)

در این زمینه، پدر تفکر استراتژیک مدرن کارل فون کلاوزویتس[9]، در رساله اصلی خود با عنوان «در مورد جنگ»[10] به آنچه دیگران متعاقباً غبار جنگ[11] نام‌گذاری کرده‌اند اشاره می‌کند تا فقدان اطلاعاتی که فرمانده در جنگ به آن‌ها نیاز دارد را توصیف کند. در این راستا ساخت یک تصویر هوشمندانه از مقصود، ساختار نیرو،

1. The Force of Ambiguity
2. Interference and Influence Operations
3. Legitimate Retaliation
4. Nuclear Strategy
5. John Baylis
6. British Nuclear Strategy
7. Deliberate Ambiguity
8. Unintentional Ambiguity
9. Carl von Clausewitz
10. On War
11. Fog of War

توانایی‌های تسلیحاتی دشمن و غیره همچنان یک قسمت مهم در هر استراتژی است. جنگ ترکیبی غبارآلودترین شکل جنگ را با توجه به ابهام عمدی که در مخفی کردن هویت کشور مهاجم دارد را نشان می‌دهد. به هر حال ندانستن این‌که دشمن دقیقاً چه کشوری است، بنیادی‌ترین چالش‌ها را برای فرمول‌بندی استراتژیک نشان می‌دهد .(Mumford, 2020:5)

نتیجه‌گیری

واقعیت این است که امروزه در حوزه نظری و عملی، نوعی سردرگمی در تعریف و تشخیص جنگ‌های نوینی چون جنگ اطلاعاتی، جنگ سایبری، جنگ ترکیبی و جنگ شناختی وجود دارد. به‌واقع همین تنوع گسترده اسامی جنگ‌های نوین در کنار شباهت‌های مفهومی و مصداقی گسترده‌ای که دارند، خود گویایی وضعیت بغرنج موجود در تعریف و تشخیص جنگ‌های نوین است. به همین دلیل برخی تلاش می‌کنند از یک تعبیر به‌عنوان‌مثال جنگ ترکیبی 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. به‌عنوان نمونه یک عملیات سایبری خرابکارانه درنهایت یک جنگ سایبری مشخص است که آن را نمی‌توان ذیل عنوانی دیگر چون جنگ ترکیبی قرار دارد. 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 مشکل است. البته در تمامی جنگ‌های نوین یک ویژگی کاملاً مشترک وجود دارد که می‌توان آن را کلید فهم مفهومی و مصداقی و همچنین آمادگی برای برتری در راه‌اندازی 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 در شکل‌گیری یا تکامل آن‌ها است. درواقع فناوری‌های نوین هم جنگ‌های نوینی چون جنگ سایبری را شکل داده‌اند و هم جنگ‌های گذشته همچون جنگ اطلاعاتی 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 به‌واسطه فناوری است و دانش‌های نوین همچون دانش سایبری و به‌ویژه هوش مصنوعی در حال تغییر بنیادین مفهوم و محتوای مخاصمه و جنگ در عرصه روابط بین‌الملل است. بر این اساس تنها راه آمادگی برای جنگ‌های نوین، در پیشگامی در علم و دانش است.

فهرست منابع

الف) منابع فارسی

ترابی، قاسم و طاهری‌زاده، محمدناصر (۱۴۰۰). «انقلاب سایبری و تحول مفهوم جنگ اطلاعاتی در عرصه روابط بین‌الملل»، **فصلنامه مطالعات بین‌المللی**، سال ۱۷، شماره ۴(۶۸)، بهار.

رزنیک، برایان (۱۳۹۷). «انتشار اخبار جعلی توییتر کار کیست»، قابل‌دسترس در:

http://www.taadolnewspaper.ir

سیگر، الیزابت (۱۳۹۹). «بزرگ‌ترین تهدید امنیتی در عصر پساحقیقت؛ چرا رساندن اطلاعات دقیق به مردم روزبه‌روز سخت‌تر می‌شود؟»، قابل‌دسترس در:

https://www.bbc.com/persian/magazine-56112997

ب) منابع انگلیسی

Bernal, Alonso and Others(2020), Cognitive Warfare on Attack Truth Thought, at:https://www.innovationhub-act.org/sites/default/files/202103/Cognitive%20Warfare.pdf

Blagovest, Tashev(2019), Russia's Information Warfare Exploring the Cognitive Dimension, at: https://www.usmcu.edu/Portals/218/CAOCL/files/RussiasInformationWarfare_MCUJ_Fall2019.pdf?ver=2019-11-19-093543-040

Brian, Lewis (2021), Information Warfare, at: https://fas.org/irp/eprint/snyder/infowarfare.htm

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

Cunningham, Conor (2020), A Russian Federation Information Warfare Primer, at: https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/#_ftnref5

Cyber Warfare (2021), at: https://www.rand.org/topics/cyber-warfare.html

Cyberwarfare (2021), at: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberwarfare.html

Green. Kieran (2020), Does War Ever Change? A Clausewitzian Critique of Hybrid Warfare, at: https://www.e-ir.info/pdf/87895

Information Warfare (2005), at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

Lewis Internet Users, (2021), at: https://www.internetlivestats.com/internet-users/
Johns Hopkins University & Imperial College London (2021), Countering cognitive warfare: awareness and resilience, at: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html
Gregory, Jennifer (2021), Quantum Security and AI: Building a Future Together, at:https://securityintelligence.com/articles/quantum-security-artificial-intelligence-future-together/
Military intelligence training (2021), at: https://www.groupedci.com/offers/military-intelligence-training/
Mumford,Andrew (2020), Ambiguity in hybrid warfare, at: Https://www.hybridcoe.fi/wp-content/uploads/2020/09/202009_Strategic-Analysis24-1.pdf
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
Ramlee Sulaiman (2005), information warfare, at: https://www.giac.org/paper/gsec/1870/information-warfare/103284
Ranger, Steve (2018), what is Cyberwar? Everything you Need to Know About the Frightening future of Digital Conflict, at; https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/
Rolington, Alfred (2013), Strategic Intelligence for the 21st Century: The Mosaic Method. Oxford University Press.
Rosencrance, Linda (2019), Cyberwarfare, at: https://searchsecurity.techtarget.com/definition/cyberwarfare
Seger, Elizabeth, Avin, Shahar and others (2020), Tackling Threats to Informed Decision-Making in Democratic Societies, Promoting Epistemic Security in a Technologically-Advanced World, at: https://www.turing.ac.uk/sites/default/files/2020-10/epistemic-security-report_final.pdf
Sheldon, John (2021), Cyberwar, at: https://searchsecurity.techtarget.com/definition/cyberwarfare
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
Tabansky, Lior (2011), Basic Concepts in Cyber Warfare, at: http://book.itep.ru/depository/cyberwar/1308129610.pdf.
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
Thiele, Ralph (2020), Artificial Intelligence –A Key Enabler of Hybrid Warfare. at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf
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/