**دیپلماسی عمومی و امپریالیسم فرهنگی امریکا در فضای سایبر**

دکتر فؤاد ایزدی[[1]](#footnote-1)/ مهسا ماه‌پیشانیان[[2]](#footnote-2)

**چکیده**

جنگ سایبری ابزار نوین دیپلماسی عمومی امریکا غرب برای ضربه زدن به مشروعیت نظام سیاسی، وحدت و تمامیت، اعتماد و وفاق ملی است؛ زیرا از این طریق می‌تواند با ایجاد اخلال در زیرساخت‌های حیاتی و سایبری کشوری میزان رضایت مردم نسبت به کارایی نظام را کاهش و با خلق بحران مشروعیت زمینه انفعال یا براندازی سیستم سیاسی مورد نظر خود را بدون درگیری نظامی و گشوده شدن آتش فراهم کند. بنابراین می‌توان گفت جنگ سایبری امروزه به‌عنوان یکی از راهکارهای نوین دیپلماسی عمومی، وسیله‌ای برای مدیریت اذهان و قلوب مخاطبان جامعه هدف در راستای اهداف سیاست خارجی این کشور است. در همین راستا، مقاله حاضر درصدد پاسخگویی به این سؤال اصلی می‌باشد که انقلاب اطلاعاتی و سایبری چگونه در خدمت دیپلماسی عمومی و امپریالیسم فرهنگی امریکا برای براندازی حکومت‌های رقیب قرار گرفته است؟ برای پاسخ به این سؤال با بهره‌گیری از نظریه‌هایی که در زمینه دیپلماسی عمومی امریکا و ارتباط آن با امپریالیسم فرهنگی ارائه شده، این فرضیه مطرح می‌شود که امریکا با بهره‌گیری از راهکارهای دیپلماسی عمومی در فضای سایبر، با ایجاد اختلال در زیرساخت‌های حیاتی یک کشور در کنار بهره‌گیری از روش‌های اقناعی بینش، بصیرت، آگاهی، اعتماد و رضایت مردم جامعه و مشروعیت نظام سیاسی را هدف قرار می‌دهد.

**واژگان کلیدی:** فناوری سایبر، دیپلماسی عمومی، امپریالیسم فرهنگی، جنگ سایبری، عملیات‌های اطلاعاتی.

**طرح مسئله**

اگرچه در طول تاریخ بشر، مبادله تجارب تاریخی، ایده‌ها، ارزش‌ها، سنت‌ها و کالاهای فرهنگی میان ملت‌های جهان سابقه‌ای دیرینه دارد، اما در هیچ دوره‌ای به‌اندازه امروز امریکا نتوانسته با کمک انقلاب اطلاعاتی و سایبری در چارچوب دیپلماسی عمومی به تبلیغ سیاسی ارزش‌های فرهنگی خود در راستای براندازی رقیبان و حریفان سیاسی گام بردارد. در دنیای کنونی، امریکا نه‌تنها با بهره‌گیری از شبکه‌های جهانی رسانه‌ای و ماهواره‌ای قادر است ارزش‌ها، هنجارها و سبک زندگی مورد نظر خود را به جهانیان القاء کند، بلکه با کمک فناوری‌‌های سایبری توانسته در راستای براندازی حکومت‌های مورد نظر نیز تلاش نماید. بنابراین، می‌توان گفت امروزه تکنولوژی‌های سایبری به‌مثابه ابزاری در خدمت امپریالیسم فرهنگی امریکا به‌کار می‌رود.

امپریالیسم فرهنگی[[3]](#footnote-3)، نشان‌دهنده نوعی نفوذ اجتماعی است كه از طريق آن كشوری بنیان‌ها، تصورات، ارزش‌ها، معلومات و هنجارهاي رفتاري و نيز روش‌هاي زندگي خود را به كشورهاي ديگر تحميل مي‌كند. این نوع امپریالیسم همچنین دربرگیرنده اشکالی متفاوت همچون امپریالیسم خبری، رسانه‌ای، اطلاعاتی و سایبری هم است.

در همین باره، امروزه امریکا می‌کوشد در چارچوب شیوه‌های متفاوتی همچون دیپلماسی عمومی؛ ارزش‌ها، سبک ‌زندگی و ایدئولوژی‌های مورد نظر خود را به کشورهای مورد نظرش انتقال دهد. در واقع، می‌توان گفت امریکا توانسته با بهره‌گیری از شبکه‌های جهانی رسانه‌ای و ماهواره‌ای به زندگی روزمره همه مردم جهان نفوذ کند. برهمین اساس است که در دوران کنونی، بیشتر امپریالیسم فرهنگی به‌معنای گسترش سلطه و هژمونی جهانی فرهنگ امریکا با هدف فرسایش و محو سنت‌ها و ارزش‌های ملی و محلی ملت‌های جهان و ظهور ارزش‌های فرهنگی امریکایی تعریف می‌شود.

علاوه‌براین، امریکا که از جنگ اول جهانی تاکنون توجه خاصی به دیپلماسی عمومی مبذول داشته، در سال‌های اخیر نیز کوشیده است با کمک وزارت دفاع و نیروی نظامی خود نقش گسترده‌ای را برای برقراری ارتباط با مردم کشورهای خارجی بازی کند. به‌خصوص اینکه با تحول سریع ارتباطات اینترنتی و اهمیت‌ یافتن فضای سایبر، این کشور درصدد بهره‌گیری از چنین فضای جدیدی در کنار شیوه‌های سنتی دیپلماسی عمومی به‌خصوص برای رقابت در عرصه جنگ شبکه‌ای با حریفان خود است. انقلاب فناوری و سایبری، توسعه رسانه‌های جدید، جهانی‌شدن، گسترش مشارکت مردم در روابط بین‌الملل و اهمیت‌یافتن مسائل بسیار پیچیدة فراملی از مهم‌ترین محرکه‌های دیپلماسی عمومی امریکا در دوران فعلی است. در این راستا، کنترل اطلاعات از نظر کارشناسان امنیتی در بالا بردن توانمندی امریکا در عرصه دیپلماسی عمومی نقشی حیاتی ایفا کرده و شبکه‌های ارتباطی و رایانه‌ها به‌لحاظ عملیاتی از اهمیت بالایی برای آن برخوردار هستند.

عملیات‌های جنگ سایبر، طیفی از شیوه‌ها را جهت تأثیرگذاری بر توانایی دشمن برای جنگ ارائه می‌دهند، به‌گونه‌ای که کشوری را قادر به نفوذ در شبکه دشمن، دسترسی به فایل‌ها، اشاعه اطلاعات نادرست یا شناخت ضعف‌های موجود در سیستم‌های آن می‌سازد. این نوع عملیات‌ها همچنین توانایی کنترل شبکه‌های دشمن به‌منظور از کار انداختن موقت یا دائمی زیرساخت‌های آن ‌را فراهم می‌آورد. علاوه‌براین، می‌توانند دشمن را از زیرساخت‌های اساسی، همچون ماهواره‌های ارتباطاتی که پشتیبان اقدامات نظامی آن هستند، محروم گرداند. یکی دیگر از مزیت‌های عملیات‌جنگ سایبر آن است که اغلب با کمترین خسارات جانبی به‌نسبت جنگ سنتی می‌توان به نتایج دلخواه دست یافت؛ برای نمونه نفوذ به سیستم‌های شبکه برق دشمن و از کار انداختن آن به‌جای بمباران تأسیسات فیزیکی این شبکه(شاپ، 2009).

برهمین اساس، امریکا به‌منظور حفظ سلطه کامل خود بر سیستم جهانی، با هم‌سطح قرار دادن راهبرد‌های رسانه‌ای و اطلاعاتی با قدرت نظامی متعارف، دکترین مبسوطی را در مورد عملیات‌های جنگ سایبر و عملیات اطلاعاتی در سال‌های 2003 و 2006 اتخاذ کرد.

 شبکه‌های ارتباطات غیرنظامی همانند اینترنت هم نقش بسیار مهمی در جنگ سایبر و عملیات اطلاعاتی داشته و برای بازبینی، کنترل و جنگ اطلاعاتی مورد استفاده قرار می‌گیرند. به‌یقین چنین مسئله‌ای باعث فرسایش انفکاک ساختاری روابط رسانه‌ای، دیپلماسی عمومی و نظامی شده و با توجه به افزایش پیچیدگی صنایع نظامی و تبلیغات رسانه‌ای در امریکا، روابط بین بخش نظامی، دولتی و بازرگانی در این کشور از پیچیدگی خاصی برخوردار شده است(برستون، 2003، صص 75-163).

در تعریف عملیات اطلاعاتی می‌توان گفت این عملیات‌ها که جنگ را با واقعیت‌های پیچیده قدرت نرم همراه می‌سازند، به جمع‌آوری، شکل‌بخشی، تجزیه و تحلیل و اشاعه بی‌وقفه اطلاعات تا تخریب توانمندی رقیب در این زمینه‌ها می‌پردازد(آرمیستید، 2004، ص19) هدف نهایی و اصلی آنها نیز کسب سلطه در قلمرو اطلاعات است. البته کسب برتری در عملیات اطلاعاتی دربرگیرنده اهدافی همچون دست‌یابی به موفقیت‌ها و برتری نظامی در عرصه زمین، هوا، فضا، دریا و عملیات‌های ویژه نیز می‌شود(نقشه راه عملیات‌های اطلاعاتی وزارت دفاع امریکا، 2003، ص4).

یکی از تحولات بسیار مهمی که در عرصه عملیات‌های اطلاعاتی رخ داده، توجه و تلاش امریکا برای ارتقای قدرت نرم خود در این زمینه است. در قدرت نرم تلاش می‌شود از طریق روش‌های اقناعی و نه اجبار، طرف مقابل مطابق با خواسته‌های ما رفتار نموده و ارزش‌ها و سیاست‌های ما را بپذیرد(نای، 2004، ص5). امریکا می‌کوشد با تقویت قدرت نرم خود برای نظام جهانی ارزش‌های مشترک فرهنگی ایجاد نموده و جوی فکری را شکل دهد که همه این ارزش‌ها را بپذیرند(فِرِیزِر، 2003، ص32).

در همین راستا، این کشور پس از 11 سپتامبر 2001، گام‌های جدی در زمینه تقویت قدرت نرم و بالا بردن قابلیت‌های عملیات اطلاعاتی خود در کشورهای مختلف جهان به‌خصوص کشورهای اسلامی برداشت. افزایش بودجه و تعداد کارشناسان عرب و ایرانی‌تبار در شبکه رادیو- تلویزیونی صدای امریکا، گسترش همکاری دانشگاه‌ها و مراکز فکری امریکایی با کارشناسانی از کشورهای اسلامی، ایجاد مراکز اطلاعاتی با ائتلاف امریکا و انگلیس در اسلام‌آباد به‌منظور مقابله با جنگ اطلاعاتی طالبان، ایجاد رادیو فردا که به‌طورمستقیم بر ایران تمرکز دارد و ایجاد شبکه رسانه‌ای خاورمیانه که شامل تلویزیون الحره[[4]](#footnote-4) و رادیو سوا[[5]](#footnote-5) می‌شود از جمله این اقدامات می‌باشد(رابرستون، 2006).

در میان این اقدامات، افزایش نظارت امریکا بر تولیدات رسانه‌ای و افزایش عملیات تبلیغاتی چشمگیرتر بود. علاوه‌براین، تبلیغات این کشور بیشتر تحت نظارت شرکت‌های خصوصی قرار گرفت. چنین مسئله‌ای سبب شد تا تمایز بین تبلیغات و جنگ روانی مبهم شود(شولمن، 2006، ص11). در واقع چنین مسئله‌ای خواسته واقعی گروهی از هواداران عملیات‌های اطلاعاتی در امریکا بود که خواهان هماهنگی دیپلماسی، تبلیغات و عملیات روانی با یکدیگر بودند. البته این ایده به‌شدت مورد مخالفت وزارت خارجه و پنتاگون قرار گرفت. زیرا اعضای این دو نهاد معتقد بودند که در صورت برقراری ارتباط بین دیپلماسی و عملیات‌های تبلیغاتی، اعتبار آنها به‌شدت مخدوش می‌شود (نقشه راه عملیات‌های اطلاعاتی وزارت دفاع امریکا، 2003، صص23-25).

اگرچه مطابق با آنچه گفته شد امریکا می‌کوشد با کنترل فضای اطلاعاتی جهان و طراحی جنگ‌های سایبری و عملیات‌های اطلاعاتی سلطه روبه افول خود در عرصه اقتصادی را جبران کند، اما واقعیت‌های مختلف نشان می‌دهد که این کشور در عرصه اطلاعاتی نیز چندان موفق عمل نکرده است. برای نمونه، به‌دنبال ناامنی‌ها و مشکلات مختلف سیاسی، اقتصادی و اجتماعی که پس از اشغال افغانستان و عراق به‌وجود آمد، امریکا برای سرپوش گذاشتن بر اقدامات خود به گسترش ظاهری دمکراسی و آزادی در خاورمیانه پرداخت. اما برخلاف این تلاش‌های صوری، موقعیتش در بین بیشتر کشورهای خاورمیانه هر روز بدتر و بدتر شد(هیئت علمی دفاعی، 2004، صص44-6). در واقع سیاست‌ها و اقدامات این کشور به‌وسیله اکثریت کشورهای اسلامی به‌عنوان تهدیدی برای موجودیت و بقای اسلام شناخته شد. از دید مسلمانان جهان، امریکا مجرمی است که با این اقدامات درصدد تحکیم سلطه خود بر خاورمیانه و تضعیف جهان اسلام برآمده است(هیئت علمی دفاعی، 2004، ص35). بنابراین می‌توان گفت اگرچه امریکا برای حفظ سلطه جهانی خود به عملیات جنگ سایبری و عملیات اطلاعاتی روی آورده، اما در مبارزه برای تصرف قلوب و اذهان با شکست سختی روبرو شده است. با ‌وجود این، علیرغم تمام مشکلاتی که در زمینه عملیات جنگ سایبر و عملیات اطلاعاتی با آن رو به‌روست، همچنان تلاش می‌نماید تا با کسب برتری در این زمینه با رقیبان جهانی خود مقابله کند.

با این توضیح، در مقاله حاضر تلاش می‌شود ضمن ارائه تعریفی از مفهوم، ماهیت و ویژگی‌های فضا و جنگ سایبر به بررسی نحوه کاربرد عملیات جنگ سایبر و عملیات اطلاعاتی برای پیشبرد اهداف دیپلماسی عمومی و امپریالیسم فرهنگی امریکا پرداخته شود.

**چارچوب نظری: دیپلماسی عمومی و امپریالیسم فرهنگی در فضای سایبر**

فناوری ارتباطات و اطلاعات يكي از مقتدرترين نيروها در شكل دادن به قرن بيست‌ويكم بوده و تغييرات اساسي حاصل از آن، در روش زندگي افراد، آموزش، كار و نيز روش حكومت دولت‌ها تأثير مي‌گذارد. در واقع، عصر حاضر را باید تلفیقی از ارتباطات و اطلاعات دانست؛ عصری که بشر در آن بیش از گذشته خود را نیازمند برقراری ارتباط برای کسب اطلاعات مورد نیاز می‌داند. ترديدي در اين واقعيت نمي‌توان داشت كه جهان درحال خيز تازه‌ای به ‌سوی يك تحول دوران‌ساز است. جانمايه اين تحول در حوزه اطلاع‌رساني و دانايي استقرار يافته است. تغییراتی که اکنون به‌واسطه انقلاب ارتباطات و فناوری‌های نوین اطلاعاتی سراسر دنیا را درمی‌نوردد، اگرچه می‌تواند به ايجاد جامعه‌اي علمي متنهي ‌شود كه در آن، جريان پيوسته اطلاعات، انتشار سريع عقايد و افكار صورت می‌پذیرد و تأثیراتی مثبت نیز در زمینه سیاسی، اقتصادی و اجتماعی دارد، اما به همان نسبت ماهیت و روش‌های تهدیدات، دیپلماسی عمومی، جنگ و براندازی را با تغییرات اساسی رو به‌رو نموده است. در این میان، دیپلماسی عمومی به شیوه‌های متفاوتی تعریف شده و در مفهومی وسیع، برای توضیح روش‌های حکومتی جهت هدایت سیاست خارجی و تأمین منافع ملی ازطریق ارتباط مستقیم با مردم یک کشور خارجی به‌کار می‌رود. فعالیت‌های این نوع دیپلماسی اشاعه اطلاعات در میان مردم کشورهای خارجی از مجرای تبلیغات، دیپلماسی فرهنگی، رسانه‌ها، اینترنت، کتابخانه‌ها و برنامه‌های مبادله اطلاعات و دانش است.

بي‌طرفانه‌ترين تعريف از ديپلماسي عمومي، آن ‌‌را اينگونه تعريف مي‌کند: «فرايندي دولتي از برقراري ارتباط با مردمان خارج در راستاي ايجاد فهمي از ايده‌ها و آرمان‌ها، نهادها و فرهنگ، نيز اهداف سياسي و خط‌مشي‌هاي ملت خود» (تاچ، 1990، ص8). در این رابطه، کميسيون مشورتي ديپلماسي عمومي امريکا[[6]](#footnote-6) با بیان اینکه هدف اصلی ديپلماسي عمومي 'ترويج سياست‌ها' است آن‌ را بدین‌صورت تعریف می‌کند: «فرايند اطلاع‌رساني، تعامل و تأثيرگذاري بر مردمان کشورهاي خارجي؛ به‌گونه‌اي‌که مردم آن کشورها در نتیجة این فعالیت‌ها، حکومت‌های خود را ترغیب به حمایت از سیاست‌های کلیدی امریکا کنند»(کمیسیون مشورتی ایالات متحده در باب دیپلماسی عمومی، 2005). در مواردي، مانند آنچه در مورد کوبا و جمهوري اسلامي ايران وجود دارد، هدف ديپلماسي عمومي امريکا از اين فراتر رفته و به تغيير حکومت معطوف مي‌شود(گیلبوا، 2006).

کريستوفر راس[[7]](#footnote-7)، مشاور ارشد معاون وزير امور خارجه در مسائل ديپلماسي عمومي و سفير سابق امريکا در سوريه و الجزاير، ديپلماسي عمومي را شبيه اقدامات ديپلماتيک مي‌بيند، با اين تفاوت که تنها دو طرف آن فرق مي‌کنند: درحالي‌که ديپلماسي سنتي دربرگيرندة "تعامل" ميان نمايندگان دو حکومت است، ديپلماسي عمومي شامل پيشبرد منافع ملي يک کشور ازطريق تعامل با طرف‌هاي غيردولتي در ديگر کشورهاست. راس بر آن است که ديپلماسي عمومي برخلاف تبلیغات سیاسی[[8]](#footnote-8) مشتمل بر فريب‌کاري براي در دست گرفتن افکار و رفتار مردم نيست(هس و کالب، 2003، ص224). او همچنين ادعا مي‌کند که ديپلماسي عمومي دربارة گفتن حقيقت است، حال ‌آنکه تبلیغات سیاسی درجاتي از دروغ‌پراکني را در خود دارد.

جوزف ناي[[9]](#footnote-9)، ديپلماسي عمومي را ابزار قدرت نرم[[10]](#footnote-10) ‌‌قدرتي اقناعي مبتني بر جاذبه‌هاي خود که براي جلب موافقت عمومي طراحي شده است ‌مي‌بيند(نای، 2004، ص5). به ‌باور وی، قدرت نرم امريکا "توانايي اين کشور براي جذب ديگران با مشروعيت‌بخشي به سياست‌هاي آن و ارزش‌هايي که اساس اين سياست‌ها هستند"، مي‌باشد(نای، 2004، ص3). بر اين اساس، قدرت نرم تنها«به‌دلیل مقبولیتی گذرا اهميت ندارد؛ بلکه ابزاري است براي رسيدن به نتايجي که امريکا خواستار آن است»(نای، 2004، ص3).

در واقع می‌توان گفت دیپلماسی عمومی امریکا دربرگیرنده تلاش‌هایی برای رابطه مستقیم با شهروندان، رهبران غیرنظامی، نخبگان، روزنامه‌نگاران و رهبران فکری یک جامعه خارجی است. ابزار این نوع دیپلماسی نیز شامل ارتباطات متقابل مردم یک کشور خارجی با امریکا، برنامه‌های کارشناسی، دیپلماسی فرهنگی، کتاب‌ها و مقالات، رادیو و تلویزیون، تبلیغات و فیلم‌ها و در دوران کنونی اینترنت و فضای سایبر می‌شود.

کتی فيتزپاتريک[[11]](#footnote-11) می‌گوید مفهوم‌پردازي ديپلماسي عمومي به ‌مثابة قدرت نرم، از منظر اخلاقي نقایصی دارد(فیتزپاتریک، 2006، ص1). برهمین اساس می‌توان گفت سياست‌هاي فرهنگي امريکا(به ‌منزلة ابزار ديپلماسي عمومي) ناشي از پيش ‌فرض‌هاي هژمونيک ‌هستند که برخي منتقدان آن‌را در حد "امپرياليسم فرهنگي" مي‌دانند(مرلیس، 2006).

امپریالیسم امریکا در دنیای پس از جنگ سرد نقابی فرهنگی به چهره زده و با عناوینی جدید همچون امپریالیسم نو[[12]](#footnote-12)، امپریالیسم نرم[[13]](#footnote-13) و امپریالیسم اقتصادی[[14]](#footnote-14) معروف شده است. در سال‌های اخیر نیز امپریالیسم فرهنگی شامل امپریالیسم رسانه‌ای[[15]](#footnote-15)، امپریالیسم ساختاری[[16]](#footnote-16)، امپریالیسم ایدئولوژیکی[[17]](#footnote-17)، امپریالیسم ارتباطی[[18]](#footnote-18)، وابستگی فرهنگی[[19]](#footnote-19) و امپریالیسم سایبری[[20]](#footnote-20) می‌شود(وایت، 2001). اگرچه این تئوری‌ها هرکدام به روشی امپریالیسم فرهنگی را توضیح می‌دهند، اما ارائه تعریفی مشخص از این مفهوم کاری بسیار پیچیده و دشوار است. با وجود این، در سال 1976 هربرت شیلر[[21]](#footnote-21) در اثر خود به‌نام "ارتباطات و سلطه فرهنگی[[22]](#footnote-22)، امپریالیسم فرهنگی را به‌عنوان روش و شیوه اصلی شرکت‌های چند ملیتی و بنگاه‌های اقتصادی سرمایه‌داری، از جمله شبکه‌های رسانه‌ای، برای توسعه تسلط و نفوذ فرهنگی خود بر کشورهای درحال توسعه تعریف کرد.

اگرچه شیلر خود بیشتر بر جنبه‌های ارتباطاتی امپریالیسم فرهنگی تأکید دارد، اما تئوری وی برای توضیح این مقوله در زمینه‌هایی دیگر همچون روابط بین‌الملل، آموزش، تاریخ و ورزش نیز کاربرد دارد. شیلر بیان می‌دارد که امپریالیسم رسانه‌ای- فرهنگی به‌عنوان زیرمجموعه‌ای از سیستم کلی امپریالیسم جهانی است(وایت، 2001). وی در جایی دیگر می‌گوید که وسایل ارتباط جمعی، بنگاه‌های عامل برای بسط سلطه فرهنگی و در نتیجه تحقق امپریالیسم فرهنگی هستند(شیلر، 1969).

بر اساس مفروضات نظریه امپریالیسم فرهنگی، نفوذ فرهنگ غرب و امریکا به سراسر جهان نه به‌علت محبوبیت و کیفیت آن، بلکه به‌علت پول و قدرت آن‌ها می‌باشد.

به‌رغم اينکه قدرت‌هاي استعماري در اواخر قرن نوزدهم کماکان از سرکوب و تحميل براي محو يا تحت انقياد درآوردن فرهنگ‌هاي بومي استفاده مي‌کردند، رويکرد تازة اين عصر جديد امپراتوري، بهره‌گیری از وسايل کمتر بي‌رحمانه براي انتقال فرهنگ بود. پيشرفت‌هاي فناوری و آموزش رسمي، بسياري از مردم بومي را نیز به سبک زندگي و انديشيدن اروپايي جذب کرد(لنسفورد، 2007). در نتيجه، امپرياليسم فرهنگي با شروع اين دوره، به اشکال واضح‌تر تهديد، ابزارهاي اقناعي را براي گسترش سلطة خود افزود و هم‌اکنون با کمک شیوه‌های نوین ارتباطی و سایبری در راستای براندازی نرم رقیبان امریکا عمل می‌کند.

**جنگ در فضای سایبر**

برای شناخت بهتر چگونگی عملکرد امریکا در عملیات‌های جنگ سایبر، باید متن حاضر را با پاسخ به این سؤال شروع کرد که «جنگ سایبر»[[23]](#footnote-23) چیست؟ با این‌حال، برای درک صحیح تعریف جنگ سایبر باید پیش از آن فضای سایبر را شناخت.

در همان‌حال که اجماع‌نظری بین‌المللی از تعریف فضای سایبر[[24]](#footnote-24)‌وجود ندارد، با تعاریف بی‌شماری از این اصطلاح مواجه هستیم. وزارت دفاع امریکا فضای سایبر‌ را به‌عنوان "حوزه‌ای جهانی در محیط اطلاعات" می‌داند که "شامل شبکه‌هایی به‌هم وابسته از زیرساخت‌های فناوری اطلاعاتی از جمله اینترنت، ‌شبکه‌های ارتباطاتی راه دور، سیستم‌های رایانه‌ای و کنترل‌کننده می‌شود"(رؤسای ستاد مشترک، 2001). توماس وینگفیلد[[25]](#footnote-25)، در کتاب خود با عنوان قانون نبرد اطلاعاتی: قانون امنیت ملی در فضای سایبر[[26]](#footnote-26)، تعریفی ساده‌تر ارائه می‌دهد: «فضای سایبر یک مکان فیزیکی نیست - به‌لحاظ بُعد فیزیکی یا طیف زمانی هم قابل سنجش نیست. فضای سایبر اشاره به محیطی دارد که از ترکیب و یکی‌شدن شبکه‌های کامپیوتری، سیستم‌های اطلاعاتی و زیرساخت‌های ارتباط از راه دور ایجاد شده که از آن به‌عنوان شبکه گسترده جهانی[[27]](#footnote-27) یاد می‌شود»(وینگفیلد، 2000). مرکز پژوهش‌های کنگره[[28]](#footnote-28) امریکا نیز در سال 2001 فضای سایبر را به‌عنوان "تمامی ارتباطات موجودات بشری از طریق رایانه‌ها و فناور‌های ارتباط از راه‌ دور بدون توجه به جغرافیای فیزیکی" تعریف کرد(شاپ، 2009).

تعاریف یادشده از فضای سایبر نشان از دشواری در تعریف این واژه دارد که به‌نوبه خود یکی از مشکلات در ایجاد اجماع‌نظر میان کشورها در رابطه با چگونگی کاربرد حقوق بین‌الملل برای جنگ در فضای سایبر است. با این‌ حال، در راستای تحلیل عملیات‌ نظامی در فضای سایبر، باید کار را با تمرکز در وهله نخست بر شبکه‌های رایانه‌ای آغاز کرد. بنابراین، با توجه به هدف مقاله حاضر، از تعریف صورت‌گرفته از فضای سایبر در استراتژی نظامی ملی[[29]](#footnote-29) امریکا استفاده می‌شود: «حوزه‌ای با ویژگی بهره‌گیری از رایانه‌ها و دیگر تجهیزات الکترونیک برای ذخیره‌سازی، ‌تغییر و تبادل داده‌ها از طریق سیستم‌های شبکه‌ای و زیرساخت‌های فیزیکی مربوطه»(لوپز، 2007).

در بارة جنگ سایبر نیز هیچ اجماع ‌نظری وجود ندارد. وزارت دفاع امریکا عملیات‌های سایبر[[30]](#footnote-30) را "به‌کارگیری توانمندی‌های سایبر در جایی" می‌داند که "هدف اصلی کسب نتایج نظامی در فضای سایبر یا ازطریق آن است". در عین‌حال عنوان می‌دارد که چنین عملیات‌هایی شامل فعالیت‌های شبکه‌‌محور رایانه‌ای برای اجرای عملیات و دفاع از شبکه اطلاعاتی جهانی است. وزارت دفاع نیز عبارت حمله شبکه‌محور کامپیوتری[[31]](#footnote-31) را "اقداماتی با بهره‌گیری از شبکه‌های رایانه‌ای برای ایجاد اختلال، قطع سرویس، پایین ‌آوردن کیفیت یا نابودی اطلاعات در رایانه‌ها و شبکه‌های رایانه‌ای یا خود رایانه‌ها و شبکه‌ها" تعریف می‌کند(رؤسای ستاد مشترک، 2001). فرمان سیاسی 10-7 نیروی هوایی[[32]](#footnote-32) امریکا هم از عملیات‌های جنگی شبکه‌محور[[33]](#footnote-33) برای تعریف "برنامه‌ریزی و به‌کارگیری یک‌پارچه توانمندی‌های نظامی جهت رسیدن به نتایج دلخواه در سرتاسر بخش به‌هم ‌مرتبط آنالوگ و دیجیتال میدان نبرد"، استفاده می‌کند. این فرمان همچنین بیان می‌کند که عملیات‌های شبکه‌‌محور در حوزه اطلاعاتی با ترکیب سخت‌افزارها، نرم‌افزارها، ‌داده‌ها و تعاملات بشری صورت می‌پذیرد و در عین‌ حال از حمله شبکه‌محور[[34]](#footnote-34) برای تعریف "به‌کارگیری توانمندی‌های شبکه‌محور جهت نابودی، ایجاد اختلال، تضعیف یا کسب اطلاعات در شبکه‌ها یا از طریق آنها" استفاده می‌کند(نیروی هوایی ایالات متحده، 2006). مرکز پژوهش‌های کنگره نیز در سال 2001 عنوان داشت که "جنگ سایبر را می‌توان برای توصیف جنبه‌های گوناگون دفاع در برابر شبکه‌های اطلاعاتی و رایانه‌ای و حمله به آنها در فضای سایبر و نیز جلوگیری از دست‌زدن دشمن به چنین کاری مورد استفاده قرار داد"(هیلدرِت، 2001). این گزارش بیان می‌کند که یکی از ویژگی‌های بارز حمله شبکه‌محور رایانه‌ای آن است که بر جریان داده‌هایی اتکا دارد که به‌ عنوان سلاحی برای اجرای یک حمله مورد استفاده می‌گیرد، برای نمونه ارسال سیگنال دیجیتال از طریق شبکه برای کنترل‌کننده‌های رایانه‌ای[[35]](#footnote-35) برای از کار انداختن جریان برق(ویلسون، 2007). کِوین کُلمَن[[36]](#footnote-36)، از کارشناسان و مشاور مدیریت راهبردی در مؤسسه تکنولِتیکس[[37]](#footnote-37)، از نهادهای فکری در امریکا، جنگ سایبر را اینگونه تعریف می‌کند: «نبردی که از حملات یا اقدامات خصمانه و غیرقانونی علیه رایانه‌ها و شبکه‌ها در راستای ایجاد اختلال در ارتباطات و دیگر بخش‌های زیرساختی به‌مثابه سازوکاری برای وارد ساختن ضربات اقتصادی یا از کار انداختن تمهیدات دفاعی استفاده می‌کند»(کُلمن، 2008).

این تعاریف گوناگون نیز نشان از دشواری در تعریف دقیق اصطلاح جنگ سایبر دارد. با فرض اینکه عملیات نظامی در فضای سایبر را می‌توان به‌صورت یک جنگ دید، در اینجا عبارت جنگ سایبر در تحلیل طیف گسترده‌ای از عملیات‌ نظامی در فضای سایبر به‌کار گرفته شده و تعریف زیر مورد استفاده قرار می‌گیرد: «به‌کارگیری توانمندی‌های شبکه‌محور یک کشور برای ایجاد اختلال، قطع سرویس، پایین آوردن کیفیت خدمات، دستکاری یا نابودی اطلاعات موجود در رایانه‌ها و شبکه‌های رایانه‌ای یا خود رایانه‌ها و شبکه‌های کشور دیگر»(شاپ، 2009، صص121-123).

**وزارت دفاع امریکا و عملیات اطلاعاتی**

همانگونه که در ابتدای مقاله اشاره شد امروزه کنترل اطلاعات و انجام عملیات‌ اطلاعاتی به‌منظور دست‌یابی به اهداف سیاست خارجی امریکا و پیشبرد دیپلماسی عمومی این کشور به‌خصوص برای براندازی رقیبان مورد نظر خود از اهمیت بسیار زیادی برخوردار است. در واقع، این امر به‌عنوان بخشی از عملیات نظامی مطرح بوده و فرماندهی راهبردی امریکا نیز عملیات اطلاعاتی را به‌عنوان یک توانمندی نظامی حیاتی تلقی می‌کند و بر مسائلی همچون بهره‌گیری از انرژی الکترومغناطیسی، عملیات در فضای مجازی و بهره‌برداری از عملیات روانی به‌منظور تأثیرگذاری بر اطلاعات دریافتی از سوی دشمن تأکید می‌کند.

هدف از عملیات اطلاعاتی کمک به فرماندهان در تصمیم‌گیری، ارزیابی تهدیدها و مخاطرات و اخذ تصمیمات به‌موقع و مناسب است. اعتماد به اطلاعات و سرعت انتقال آن‌ا اهمیت حوزۀ اطلاعات را بیش از هر زمان دیگر بالا می‌برد. امروزه عملیات اطلاعاتی که شامل عملیات‌ نفوذ، جنگ شبکه‌ای و جنگ الکترونیک می‌شوند، زیرمجموعه‌ای از جنگ سایبر به‌‌شمار می‌رود(رؤسای ستاد مشترک، 2001). مقامات وزارت دفاع امریکا نیز هم‌اکنون فضای سایبر را در کنار زمین، هوا و دریا به‌عنوان عرصه‌ای برای نبرد تلقی می‌کنند. این وزارتخانه، اطلاعات را در جنگ به‌منزله یک سلاح و در عین‌حال به‌منزله یک هدف تلقی می‌کند. در همین خصوص، عملیات روانی[[38]](#footnote-38) امکان انتشار سریع اطلاعات اقناع‌کننده را برای تأثیر مستقیم بر فرایند تصمیم‌گیری مخاطبان ساکن در قلمرو دشمن فراهم می‌کند.

وزارت دفاع امریکا هم‌اینک از لفظ "عملیات اطلاعاتی" برای اشاره به نبرد برای کسب اطلاعات نظامی استفاده می‌کند. عملیات اطلاعاتی فعالیت‌هایی هستند که در مواقع بحران یا جنگ به‌منظور تأثیرگذاری بر اطلاعات دشمن در عین حفاظت از سیستم‌های اطلاعاتی خودی برای تحقق یا کمک به تحقق اهداف معین صورت می‌گیرند (فرهنگ لغت نظامی و اصطلاحات مرتبط وزارت دفاع، 2003). این نوع عملیات‌ به‌طور مشخص با هدف ایجاد اخلال یا تأثیرگذاری بر فرایندهای تصمیم‌گیری دشمن انجام می‌پذیرند. یک حمله مبتنی بر عملیات اطلاعاتی می‌تواند اشکالی متعدد داشته باشد که از آن‌جمله می‌توان به موارد ذیل اشاره کرد:

* پایین آوردن کارآیی رایانه‌های دشمن: امکان ایجاد اختلالات نرم‌افزاری از طریق انتقال یک ویروس یا کرم رایانه‌ای وجود دارد؛
* از کار انداختن سلاح‌های پیشرفته دشمن: در این مورد می‌توان به بالا بردن درجه حرارت مدارهای اتصال رایانه‌ای از طریق پالس‌های بالا و مستقیم انرژی اشاره کرد؛ و
* گمراه کردن حسگرهای دشمن: در این مورد نیز می‌توان به‌منظور ایجاد تصاویر جعلی اقدام به پخش سیگنال‌های بسیار قوی کرد.

از جمله سایر روش‌های انجام عملیات تهاجمی اطلاعاتی می‌توان به عملیات روانی مانند راه‌اندازی شبکه‌های رادیویی و تلویزیونی به‌منظور تأثیرگذاری بر افکار و رفتارهای مخاطبان مورد نظر یا در دست گرفتن کنترل شبکه‌های ارتباطی برای ایجاد اخلال در انسجام فرماندهی دشمن اشاره کرد.

از میان روش‌های یادشده، وزارت دفاع امریکا بیش از پیش بر تسلط روی عرصه طیف‌های الکترومغناطیسی از طریق روش‌هایی برای انجام حملات به شبکه‌های رایانه‌ای و جنگ الکترونیک تأکید دارد. این وزارتخانه همچنین بر این نکته تأکید دارد که با توجه به اینکه شبکه‌های رایانه‌ای به‌طور فزاینده‌ای به مرکز ثقل نبرد تبدیل شده‌اند، نیروهای نظامی امریکا نیز باید آمادگی لازم جهت نبرد در عرصه شبکه را به‌دست آورند(نقشه راه عملیات اطلاعاتی وزارت دفاع امریکا، 2003).

**قابلیت‌های پنج‌گانه عملیات اطلاعاتی امریکا**

وزارت دفاع امریکا پنج قابلیت حیاتی را در ارتباط با اجرای عملیات اطلاعاتی برمی‌شمرد: جنگ و عملیات روانی[[39]](#footnote-39)، فریب نظامی[[40]](#footnote-40)، امنیت عملیات[[41]](#footnote-41)، عملیات شبکه‌‌محور رایانه‌ای[[42]](#footnote-42) و جنگ الکترونیک. این قابلیت‌ها متقابلاً به یکدیگر وابسته هستند و به‌طور فزاینده‌ای به‌منظور تحقق اهداف مورد نظر با یکدیگر تلفیق می‌شوند. در ادامه به بررسی آنها ‌پرداخته می شود:

**الف) جنگ روانی**

اصطلاح جنگ روانی در سال 1941 از زبان آلمانی وارد امریکا شد. بر طبق تعریف کریستوفر سیمپسون[[43]](#footnote-43) جنگ روانی به‌معنای کاربرد علمی تبلیغات سیاسی، ترور و فشار دولتی به‌عنوان وسایلی برای تضمین پیروزی ایدئولوژیکی بر یک دشمن است(سیمپسون، 1994).

تا پیش از جنگ دوم جهانی، امریکا جنگ روانی را اقدامی ناکارآمد فرض می‌کرد. اما عرصه این جنگ زمینه‌ای برای کسب تجاربی در مورد کاربرد روش‌های مربوط به این مسئله شد(دایِتز، 2003). روان‌شناسانی که در دانشگاه‌ها یا بیمارستان‌ها فعالیت داشتند، نقشی بسیار مهم در گسترش و توسعه جنگ روانی ایفا کردند. البته مطالعاتی که در فاصله سال‌های 1945 تا 1960 به روش‌های گوناگون در زمینه وسایل ارتباط جمعی و جنگ روانی در امریکا صورت پذیرفت از اهمیت بسیار زیادی در این زمینه برخوردار است. تحقیقاتی که به‌وسیله اندیشمندان علوم اجتماعی امریکا به‌خصوص متخصصان ارتباطات جمعی صورت پذیرفت به دولت این کشور و کشورهای غربی برای تحت‌ تأثیر قرار دادن گروه‌های مورد نظر کمک بسیار زیادی کرد(گاردینر، 2003). در اواخر دهه 1950 و 1960 برنامه جنگ روانی امریکا بودجه بسیار زیادی را برای انجام تحقیقاتی در زمینه رسانه‌های جمعی اختصاص داد. اگرچه دولت امریکا نمی‌توانست تحقیقاتی که در این زمینه انجام می‌گرفت را کنترل کند، اما بر این رشته حاکمیت داشت(لانگو، 2001).

ابهام و پیچیدگی که در تعریف جنگ روانی وجود دارد، به‌وسیله گزارشی در سال 2003 توضیح داده شد. این گزارش عنوان داشت که جنگ روانی تحت‌ تأثیر نقشه راه عملیات اطلاعاتی قرار گرفته است. چنین مسئله‌ای سبب می‌شود که عملیات روانی به‌عنوان یک موضوع فرعی از عملیات اطلاعاتی قرار گیرد. با تمام ابهاماتی که در زمینه عملیات روانی وجود دارد دکترین عملیات روانی مشترک در سال 2003 این تعریف را برای این واژه پذیرفته است: «عملیات طراحی‌شده برای هدایت اطلاعات انتخاب‌شده به‌سوی مخاطبان خارجی به‌منظور تأثیرگذاری بر احساسات، انگیزه‌ها، اهداف و سرانجام رفتار حکومت‌ها، سازمان‌ها، گروه‌ها و افراد یک کشور خارجی». در همین رابطه نیز آمده است که "جنگ روانی یک بخش بسیار مهم و حیاتی از فعالیت‌های دیپلماتیک، نظامی، اطلاعاتی و اقتصادی امریکا به‌شمار می‌رود. این مفهوم در زمان جنگ و صلح برای شکل دادن به اطلاعات و تأثیرگذاشتن بر مخاطبان خارجی به‌کار می‌رود"(رؤسای ستاد مشترک، 2001). مهم‌ترین مسئله‌ای که از این تعریف مشخص می‌شود، آن است که ابزار اصلی جنگ روانی، تبلیغات سیاسی است که احساسات و رفتار مخاطبان خارجی را هدف قرار می‌دهد.

تکنیک‌های جنگ روانی هرچند از رادیو، اینترنت، تلویزیون و رسانه‌های جهانی استفاده می‌کند، ولی همین فناوری‌های بسیار مدرن، دولت و جامعه مدنی را با ابهاماتی مواجه می‌سازد که به ‌نوبة خود نگرانی‌هایی را برای زندگی اجتماعی به‌وجود آورده است(ویریلیو، 2000). برای نمونه، در عملیاتی که برای ‌نخستین‌بار به اشغال نظامی عراق منجر شد، رهبران نظامی امریکا از شبکه سی.‌‌ان.‌‌ان به‌عنوان یک ابزار مناسب برای انجام جنگ روانی ضد صدام بهره بردند. در کنفرانس رسانه‌ای که این شبکه در مورد چگونگی حمله به عراق برگزار کرد، بر اساس شیوه‌های فریب راهبردی و عملیات روانی که رهبران نظامی امریکا در این جنگ به‌کار گرفتند، صدام هرگز تصور حمله به کشورش و اشغال آن‌ را نداشته و اقدامات نیروهای نظامی امریکا را در سطح برگزاری یک مانور نظامی ارزیابی می‌کرد. در واقع، صدام حسین در دام اطلاعات غلطی افتاد که بیشتر نیروهای عراقی آن‌ را بر اساس ادراکات خود از برنامه‌های شبکه سی‌.‌ان.‌‌ان مطرح می‌کردند(بِلکناپ، 2001).

به هر ترتیب، اگرچه میزان تأثیر و کاربرد فناوری‌های رسانه‌ای بر مخاطبان خارجی چندان آشکار نیست، اما زمانی‌ که افکار عمومی داخلی با شرکت در جنگی مخالف باشد، اطلاعات نادرست و فریب که در جنگ روانی از آنها استفاده می‌شود، می‌تواند تأثیری مستقیم بر مسائل اجتماعی مختلف همانند موضوعات ملی و اقتصادی داشته باشد(پادوک و آلفرد، 1990).

یکی دیگر از مسائلی که در زمینه جنگ روانی امریکا می‌توان گفت، این است که این عملیات تنها برای مخاطبان خارجی طراحی شده و هیچ بودجه‌ای را وزارت امورخارجه این کشور برای تأثیرگذاری بر شهروندان امریکایی در نظر نگرفته است. به‌هرحال، این امکان وجود دارد که جنگ روانی در آینده، شهروندان امریکایی را هدف خود قرار دهد، زیرا تلویزیون و اینترنت که به‌عنوان ابزار این جنگ به‌کار می‌روند خود می‌توانند ایجادکننده جنگی جدید علیه شهروندان امریکایی باشند. از سوی دیگر، اگرچه امریکا می‌کوشد به سریع‌ترین و جدیدترین تکنیک‌های عملیات روانی برای تحت‌تأثیر قرار دادن مخاطبان خارجی دست یابد، اما این سلاح‌ها و تاکتیک‌های جدید تنها مخاطبان خارجی را تحت‌تأثیر قرار نمی‌دهد، بلکه تهدیدات و خطرات داخلی برای شهروندان امریکایی را نیز افزایش می‌دهد(دِردِریان، 2001).

به‌طور کلی، می‌توان گفت جنگ روانی همان ادامه جنگ سخت با ابزار و روش‌های رسانه‌ای است. رسانه‌ها امکاناتی را به وسعت جهانی برای نیروهای نظامی ایجاد نموده، پیام‌های نظامی را ارسال و مأموریت‌های آنها را عملیاتی می‌کنند. همچنین رسانه‌ها به‌عنوان منبعی برای اطلاعات و هدایت‌کننده جنگ روانی نیز به‌کار می‌روند.

**ب) عملیات روانی**

وزارت دفاع امریکا عملیات روانی را به‌عنوان عملیات برنامه­ریزی­شده برای انتقال اطلاعات گزینشی به مخاطبان خارجی مورد نظر جهت تأثیرگذاری بر عواطف، انگیزه‌ها، تفکر عینی و سرانجام رفتار دولت‌ها، سازمان‌ها، گروه‌ها و افراد خارج از کشور تعریف می‌کند(فرهنگ لغت نظامی و اصطلاحات مرتبط وزارت دفاع، 2003). برای نمونه در جریان عملیات موسوم به عملیات آزادي عراق[[44]](#footnote-44)، پیام‌هایی از طریق هوا و توسط هواپیمای ای‌سی- 130. ای.‌ای[[45]](#footnote-45) متعلق به نیروی هوایی امریکا نیز کشتی‌های نیروی دریایی مستقر در خلیج فارس همچنین ایمیل‌ها، فاکس‌ها و تلفن‌های همراه برای بسیاری از چهره‌های مهم عراقی ارسال شد که آنها را به عدم حمایت از صدام حسین تشویق می‌کرد.

در حال حاضر، وزارت دفاع امریکا بر این نکته تأکید دارد که عملیات روانی باید تقویت شده و بر فرایندهای بالقوه تصمیم‌گیری دشمن، گاه حتی خيلي بیشتر از زمان شروع نبرد، تمرکز یابد. امکانات فراهم‌شده برای اجرای عملیات روانی باید بر مبنای دانش عمیق نسبت به فرایندهای تصمیم‌گیری مخاطبان تهیه شده باشند. در مرحله بعد، این محصولات باید به‌سرعت تولید شده و در سرتاسر حوزه عملیاتی در اختیار مخاطبان مورد نظر قرار گیرند(نقشه راه عملیات‌های اطلاعاتی وزارت دفاع امریکا، 2003).

اما بر مبنای سیاست‌های تعیین‌شده ازسوی وزارت دفاع امریکا، بهره‌گیری از عملیات روانی علیه مخاطبان امریکایی ممنوع است. به‌هرحال، علیرغم آنکه محصولات مربوط به عملیات روانی با هدف تأثیرگذاری بر مخاطبان خارجی طراحی می‌شوند، وزارت دفاع امریکا به این نکته واقف است که رسانه‌های جهانی ممکن است بخشی از این تأثیرات را به خود مخاطبان داخلی این کشور انتقال دهند. بنابراین، مرز دقیقی را میان مخاطبان خارجی و داخلی در این زمینه نمی‌توان ترسیم کرد(نقشه راه عملیات‌های اطلاعاتی وزارت دفاع امریکا، ص26).

**ج) فریب نظامی**

 در فریب نظامی از طریق ارائه اطلاعات، تصاویر یا گزاره‌های کاذب، دشمن به‌ سمت تصمیم‌گیری اشتباه سوق داده می‌شود. فریب نظامی عبارت از مجموعه فعالیت‌هایی است که با هدف گمراه‌سازی طراحان و تصمیم‌گیرندگان امور نظامی دشمن در زمینه قابلیت‌های نظامی نیروهای خودی و در نتیجه سوق دادن دشمن به اتخاذ یا عدم اتخاذ تدابیری معین صورت می‌گیرد که به موفقیت عملیات نظامی نیروهای خودی کمک می‌کند. برای نمونه، در جریان عملیات حمله به عراق، نیروی دریایی امریکا از سیستم تله هوایی با هدف منحرف کردن تمرکز خطوط هوایی عراق از هواپیمای مهاجم اصلی بهره برد(ویلسون، 2007).

**د) امنیت عملیاتی**

امنیت عملیاتی عبارت است از فرایند تعیین و حفاظت از اطلاعاتی که برای عملیات نیروهای خودی اهمیت حیاتی دارند و در عین حال می‌توانند به دشمن امکان دهند تا نقاط عملیاتی آسیب‌پذیر را مورد حمله قرار دهد. برای نمونه در خلال عملیات حمله به عراق، به نیروهای امریکایی اخطار داده شد تا اطلاعات خاصی را از روی پایگاه‌های اینترنتی عمومی وزارت دفاع حذف کنند تا نیروهای عراقی نتوانند اطلاعات حساس اما طبقه‌بندی نشده را مورد استفاده قرار دهند(ویلسون، 2007).

**ه) عملیات‌ شبکه‌‌محور رایانه‌ای**

عملیات‌ شبکه‌‌محور رایانه‌ای در برگیرنده قابلیت‌هایی همچون حمله به شبکه‌های رایانه‌ای دشمن و ایجاد اخلال در آنها، حفاظت از سیستم‌های اطلاعات نظامی نیروهای خودی و بهره‌برداری حداکثری از شبکه‌های رایانه‌ای دشمن از طریق گرد‌آوری اطلاعات است که به‌طور معمول از طریق کاربرد کدها و نرم‌افزارهای رایانه‌ای صورت می‌گیرد.

فرماندهی مشترک جنگ عملیاتی اطلاعاتی[[46]](#footnote-46) و فرماندهی مشترک بخش کارکردی در باب جنگ شبکه‌‌محور مسئولیت به‌‌ روزرسانی قابلیت‌های مربوط به انجام حملات به شبکه‌های رایانه‌ای را بر عهده دارند. میزان دقیق توانایی‌های این دو سازمان، فوق‌سری و طبقه‌بندی ‌شده می‌باشد، اما بسیاری از مسئولان امور امنیت رایانه بر این باورند که آنها قابلیت تخریب شبکه‌های ارتباطی و نفوذ به رایانه‌های کشور هدف به‌منظور سرقت یا دست‌کاری اطلاعات یا حتی از کار انداختن سیستم‌های کنترل و فرماندهی دشمن را نیز دارند. همچنین این باور وجود دارد که اعضای سازمان‌های یادشده را افرادی از سازمان اطلاعات مرکزی امریکا، سازمان امنیت ملی، اف‌.‌‌بی‌.‌‌آی، چهار رکن اصلی نیروهای نظامی و نمایندگان نظامی و غیرنظامی کشورهای متحد امریکا تشکیل می‌دهند(لَسکِر، 2005).

**و) جنگ الکترونیک**

وزارت دفاع امریکا جنگ الکترونیک را به تمامی فعالیت‌هایی اطلاق می‌کند که با هدف تعیین مسیر یا کنترل انرژی طیف‌های الکترومغناطیسی به‌منظور گمراه‌ساختن یا حمله به دشمن صورت می‌گیرند. انرژی الکترومغناطیسی با شدت بالا می‌تواند به‌عنوان ابزاری برای ایجاد اضافه بار یا اخلال در مدارهای الکتریکی تقریباً تمامی تجهیزاتی که در آنها از ترانزیستور، ریزمدارها یا سیم‌پیچی فلزی استفاده شده باشد، به‌کار گرفته شود (نقشه راه عملیات‌های اطلاعاتی وزارت دفاع امریکا، 2003، ص61). سلاح‌هایی که بر مبنای تغییر جهت انرژی الکترومغناطیسی کار می‌کنند، می‌توانند قدرت یک میدان الکترومغناطیسی را از طریق ساطع کردن انرژی کافی برای سوزاندن یا ایجاد آسیب شدید به مدارهای اتصال یا از کار انداختن و تغییر جهت فرایند پردازش در سیستم‌های رایانه‌ای افزایش داده یا به‌کلی خنثی کنند. بخش جنگ الکترونیک در اداره جنگ‌های نامتقارن[[47]](#footnote-47) ارتش مسئولیت تعیین سیاست‌های مربوط به جنگ الکترونیک و نیز تقویت مبانی و مفاهیم نظری مربوط به طیف‌های انرژی الکترومغناطیسی را که می‌تواند در ساخت سلاح‌ها و تجهیزات مختلف به‌کار گرفته شود، بر عهده دارد.

**جمع‌بندی**

اهمیت اطلاعات و کنترل آن در قرن بیست‌ویکم به حقیقتی تبدیل شده است که هیچ‌کس نمی‌تواند منکر آن شود. تغییر چهره، ماهیت و شیوه‌های جنگ‌‌های مدرن و کشیده‌ شدن عرصه نبرد بازیگران دولتی و غیردولتی به فضای مجازی، ابزارهای دیپلماسی عمومی را نیز تغییر داده و جنگ سایبری را به‌عنوان یکی از روش‌های جدید در این راستا از اهمیت بسیار زیاد برخوردار نموده است. در این شیوه، ابعاد درگیری به میدان نبرد محدود نبوده بلکه به علت ترکیب عملیات نظامی با اقدامات خصمانه در عرصه اقتصادی، اجتماعی، سیاسی و دیپلماتیک حیطه آن تا قلب، ذهنیت، بینش، فرهنگ، آگاهی و وجدان عمومی جامعه هدف گسترش می‌یابد.

در واقع، با ورود به عصر اطلاعات دیپلماسی عمومی از پیچیدگی مفهومی و روشیِ بسیار زیادی برخوردار شده و از روش‌های نوینی همانند درگیری در فضای سایبر بهره می‌برد. برهمین مبنا، می‌توان جنگ سایبر را به‌عنوان مجموعه‌ای از فنون عملیاتی جدید و سبک نوینی از درگیری روانی و ذهنی تعریف کرد که در آن مناقشه‌های بسیار شدید سیاسی، اقتصادی، اجتماعی و فرهنگی به‌منظور هدف قرار دادن مشروعیت و کارآمدی نظام حکومتی به اعتماد و رضایت سیاسی مردم جامعه هدف آسیب وارد می‌سازد.

همان‌گونه‌ که در نبرد‌های نظامی سلاح‌های سخت‌افزاری موجودیت دولت هدف را مورد حمله قرار می‌دهند در جنگ سایبری نیز فناوری‌های نوین رایانه‌ای بر ماشین دولت، نهادهای مالی، زیرساخت‌های حیاتی در بخش انرژی و حمل‌ و نقل و سرانجام روحیه و عزم، اعتماد و رضایت ملی، مشروعیت و کارآیی نظام سیاسی آسیب‌های جدی وارد می‌کنند؛ زیرا مشروعیت و اعتماد سیاسی به رضایت مردم از عملکرد دولت مربوط باز می‌گردد. این مفاهیم در کل با دو عامل اصلی روند و بازده سنجیده می‌شود. بخش روند به مسائلی نظیر نحوه فرایند تصمیم‌گیری و بخش بازده به کارآمدی بیشتر دولت مربوط می‌شود. همچنین، مسئله اصلی در تمام برداشت‌های یادشده این است که مجموعه سیاست‌های اتخاذ شده به‌وسیله دولت در زمینه‌های گوناگون چه تأثیری را بر مردم جامعه گذاشته و آنها چگونه چنین مواردی را تجربه می‌کنند. به‌عبارت دیگر در بررسی این مسائل، تأکید از آثار عینی سیاست‌ها و تحولات به آثار ذهنی آنها در افراد معطوف می‌شود. بنابراین در بررسی مفهوم مشروعیت، اعتماد و رضایت سیاسی نه اوضاع و شرایط عینی بلکه ارزیابی افراد از این شرایط و احساس درونی آنها مورد توجه قرار می‌گیرد. در صورتی‌که جامعه‌ای از عملکرد دولت احساس رضایت نداشته باشد، کم‌کم نسبت به نظام حاکم بی‌تفاوت و بی‌اعتماد شده، وفاداری و حمایت آگا‌هانه‌اش از دولت کاهش یافته و آرا و نظرات خود را به صورت انزوای سیاسی، اعتراض، اعتصاب، اغتشاش، شورش و جنگ نشان می‌دهد. این شکل از بیان افکار می‌تواند با خلق بحران مشروعیت سبب بی‌ثباتی سیاسی و بحران امنیتی شود. همچنین، نارضایتی از اوضاع سیاسی، اجتماعی و اقتصادی کشور، از میزان دلبستگی ملی کاسته و با تقلیل آستانه تحمل در برابر فشارها و تهدیدها بر کنش‌های مخالفت‌جویانه شهروندان می‌افزاید. برهمین اساس، بازیگران جنگ‌های سایبری می‌توانند با خلق بحران‌های موجود، بدون نیاز به درگیری‌های نظامی به اهداف راهبردی و سیاسی خود دست یابند. در واقع، این شیوه نوین درگیری با هدف ایجاد تشویش و نگرانی روانی، اقدامات برنامه‌ریزی شده‌ای را برای انتقال اطلاعات و شاخص‌های منتخب به مخاطبان خارجی به‌منظور تغییر رفتار آنها در راستای اهداف خود یا حتی براندازی نظام مورد نظر در‌بر‌می‌گیرد. برهمین اساس می‌توان گفت چون این شیوه از جنگ به‌صورت کاملا سیاسی به‌منظور مدیریت افکار و قلوب مردم جامعه هدف در فضای سایبر سازماندهی داده شده و اهداف امنیتی، فرهنگی، اقتصادی و اجتماعی را با روش‌های اقناعی دنبال می‌کند ابزاری نوین برای دیپلماسی عمومی به‌شمار می‌رود؛ زیرا همانگونه که پیش‌تر توضیح داده شد مهم‌ترین هدف دیپلماسی عمومی نیز همین مسئله است.

در این میان، کشورهای مختلفی از جهان همچون امریکا نیز می‌کوشند برای مقابله با توانمندی‌های نامتقارن رقیبان خود در عرصه عملیات‌ جنگ سایبر و عملیات اطلاعاتی، قابلیت‌های تدافعی و تهاجمی خود را افزایش دهند. در واقع، موفقیت امریکا در این عرصه نیازمند کاربرد شیوه‌های تازه برای اعمال کنترل بر اطلاعات و جمعیت غیرنظامی جهان است که می‌توان آن ‌را شکلی جدید از امپریالیسم فرهنگی این کشور دانست. ابزار این اقدام هم در شکلی محدود و غیرمهلک عملیات اطلاعاتی و عملیات‌های جنگ سایبر است.

به‌هرحال، با توجه به گسترش فناوری‌های ارتباطاتی در سطح جهان و دسترسی همگانی به آن، اجرای چنین چیزی به آسانی امکان‌پذیر نیست و تجارب سال‌های اخیر نیز عدم امکان سلطه کامل بر اطلاعات را نشان می‌دهد.

با این توضیح، همانگونه که در بخش‌های ابتدایی مقاله نیز اشاره شد، یکی از راه‌های جدید امریکا برای پیشبرد اهداف سیاست خارجی خود که از آن به‌عنوان امپریالیسم فرهنگی یاد می‌کنیم، بهره‌گیری از فناوری‌های سایبری در راستای دیپلماسی عمومی با هدف تأثیرگذاری و در مواردی براندازی حکومت‌های رقیب(ازجمله ایران) است. برای نمونه این کشور با بهره‌برداری از قابلیت‌های فضای سایبر، تلاش دارد به هویت‌های اجتماعی مخالف نظام جمهوری اسلامی ایران شکل داده و به آنها این توانمندی را بدهد که با سوء ‌استفاده از بحران‌های اجتماعی، سیاسی و اقتصادی پدیده آمده در جامعه به مشروعیت و کارآمدی نظام سیاسی خدشه وارد آورند. شکل دادن به گروه‌های سیاسی و اجتماعات مجازی، نافرمانی مدنی، دمکراسی دیجیتالی، افکارسازی، نفوذ و خراب‌کاری، مبارزه با کنترل خبری دولتی، انسداد سایت‌ها، رفراندوم اینترنتی و ایجاد مطالبات جدید سیاسی از جمله این راهکارها محسوب می‌شود(ماه‌پیشانیان، 1389).

برهمین اساس این کشور دکترین مبسوطی را در زمینه عملیات اطلاعاتی و عملیات‌ جنگ سایبر تدوین نموده و به سازماندهی و آموزش نیروهای مورد نظر خود در این زمینه پرداخته است. بنابراین، مشخص است که نیاز به‌وجود افراد متخصص در چنین جنگی را درک نموده و در این راستا اقدام نموده است. امریکا، سرمایه‌گذاری وسیعی هم در این حوزه داشته است، ولی نسبت به موفقیت آن با توجه به چنین حجمی از سرمایه‌گذاری تردید وجود دارد. برای نمونه، علیرغم لفاظی‌های فراوان علیه ایران و به‌کارگیری امکانات فراوان برای یاری‌رساندن به مخالفان آن در عرصه سایبر و تولید ویروس‌هایی جهت خرابکاری در برنامه هسته‌ای کشورمان، موفقیتی از این اقدامات گزارش نشده است. در آخرین مورد نیز ایران توانست یکی از پیشرفته‌ترین هواپیماهای بدون سرنشین این کشور را با استفاده از جنگ سایبری و الکترونیکی به زمین نشاند. این شکست برای امریکا به‌حدی سخت بود که باراک اوباما به‌طور رسمی خواستار بازگرداندن هواپیمای یادشده شد. پیش از این نیز ایران توانست با موفقیت از آسیب رسیدن به تأسیسات هسته‌ای خود توسط ویروس‌هایی همچون استاکس‌نت جلوگیری کند.

به‌هرحال، امریکا به‌خوبی می‌داند برخلاف گذشته که تسلیحات پیشرفته تنها در انحصار قدرت‌های بزرگ بود و آنها می‌توانستند حرف آخر را در جنگ‌های فیزیکی بزنند، چنین چیزی در مورد فضای سایبر و جنگ سایبر صدق نمی‌کند، چراکه کشورها و گروه‌های دیگر نیز با داشتن تخصص لازم که به‌راحتی در همین شبکه جهانی قابل دسترسی می‌باشد، می‌توانند به شیوه‌های نوین نبرد دست یافته و دست برتر را داشته باشند. بنابراین، رسیدن به اهداف امپریالیسم فرهنگی در این حوزه برای کشوری همچون امریکا، شاید به راحتیِ بهره‌گیری از شیوه‌های سنتی نباشد.

سرانجام می‌توان گفت اگرچه امروزه امریکا برای کسب برتری جهانی می‌کوشد به سلطه اطلاعاتی و موفقیت در زمینه عملیات جنگ سایبر و عملیات اطلاعاتی دست یابد، اما عدم تفاهم سیاست‌مداران و کارشناسان این کشور در مورد تهدیدات سایبری و روش‌های مقابله با آن، افزایش توانمندی رقیبانی همچون روسیه و چین و ایران در عرصه سایبری، ماهیت سیال و نامشخص تهدیدات گروه‌های غیردولتی و تروریستی برای امنیت ملی امریکا، در بحران قرار گرفتن دیپلماسی عمومی این کشور به‌علت افول محبوبیت آن در جهان به‌خصوص در میان مسلمانان، ابهام موجود در بیانیه‌ها، دستورات و دکترین‌های مرتبط با جنگ سایبر، پیچیدگی روابط رسانه‌ای- نظامی و صنعتی، و کم‌رنگ‌ شدن مرز بین مخاطبان داخلی و خارجی در تبلیغات سیاسی این کشور به‌علت رشد رسانه‌های جهانی سبب شده است که احتمال پیامدهای مخرب عملیات جنگ سایبر و عملیات اطلاعاتی برای این کشور سخت و غیرقابل محاسبه باشد.

**منابع**

در نسخه چاپی موجود است.

1. استادیار گروه مطالعات امریکای شمالی، دانشکده مطالعات جهان، دانشگاه تهران [↑](#footnote-ref-1)
2. دانشجوی دکتری علوم سیاسی دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران [↑](#footnote-ref-2)
3. cultural imperialism [↑](#footnote-ref-3)
4. Al-Hurra TV [↑](#footnote-ref-4)
5. Radio Sawa [↑](#footnote-ref-5)
6. The U.S. Advisory Commission on Public Diplomacy [↑](#footnote-ref-6)
7. Christopher Ross [↑](#footnote-ref-7)
8. Propaganda [↑](#footnote-ref-8)
9. Joseph S. Nye [↑](#footnote-ref-9)
10. Soft Power [↑](#footnote-ref-10)
11. Kathy R. Fitzpatrick [↑](#footnote-ref-11)
12. Neo-colonialism [↑](#footnote-ref-12)
13. soft imperialism [↑](#footnote-ref-13)
14. economic imperialism [↑](#footnote-ref-14)
15. media imperialism [↑](#footnote-ref-15)
16. structural imperialism [↑](#footnote-ref-16)
17. ideological imperialism [↑](#footnote-ref-17)
18. communication imperialism [↑](#footnote-ref-18)
19. cultural dependency [↑](#footnote-ref-19)
20. cyber imperialism [↑](#footnote-ref-20)
21. Herbert Schiller [↑](#footnote-ref-21)
22. Communication and Cultural Domination [↑](#footnote-ref-22)
23. cyber warfare or cyber war [↑](#footnote-ref-23)
24. cyberspace [↑](#footnote-ref-24)
25. Thomas Wingfield [↑](#footnote-ref-25)
26. The Law of Information Conflict: National Security Law in Cyberspace [↑](#footnote-ref-26)
27. World Wide Web (WWW) [↑](#footnote-ref-27)
28. Congressional Research Service (CRS) [↑](#footnote-ref-28)
29. National Military Strategy (NMS) [↑](#footnote-ref-29)
30. cyber operations [↑](#footnote-ref-30)
31. computer network attack [↑](#footnote-ref-31)
32. Air Force Policy Directive 10-7 [↑](#footnote-ref-32)
33. network warfare operations [↑](#footnote-ref-33)
34. network attack [↑](#footnote-ref-34)
35. Controller: یکی از واحدهای اصلی در هر رایانه که فرامین برنامه‌ها را اجرا می‌کند. [↑](#footnote-ref-35)
36. Kevin Coleman [↑](#footnote-ref-36)
37. Technolytics Institute [↑](#footnote-ref-37)
38. Psychological Operations [↑](#footnote-ref-38)
39. psychological warfare & Operations [↑](#footnote-ref-39)
40. military deception [↑](#footnote-ref-40)
41. operational security (OPSEC) [↑](#footnote-ref-41)
42. computer network operations (CNO) [↑](#footnote-ref-42)
43. Christopher Simpson [↑](#footnote-ref-43)
44. Operation Iraqi Freedom (OIF) [↑](#footnote-ref-44)
45. EC-130EE [↑](#footnote-ref-45)
46. Joint Information Operations Warfare Command (JIOWC) [↑](#footnote-ref-46)
47. Asymmetric Warfare Office (AWO) [↑](#footnote-ref-47)