تحلیل شبکه‌های اجتماعی در جنگ ترکیبی

عبدالله اعتمادی‌راد[1]

چکیده

هدف از این مقاله تحلیل شبکه‌های اجتماعی، تأثیر آن‌ها بر جنگ‌های امروز، تعریف جنگ‌های ترکیبی و اثر آن‌ها بر میدان‌های جنگ است. همچنین پاره‌ای از مشخصه‌های محیط اطلاعاتی (فضای مجازی) مورد بررسی قرار می‌گیرد زیرا این مشخصه‌ها ابزارهای جنگ ترکیبی هستند که در این مقاله بررسی می‌شود.

علت بررسی مشخصه‌های فضای مجازی بارز کردن این است که چگونه از فضای مجازی می‌تواند به‌عنوان سلاح در جنگ‌های ترکیبی استفاده شود.

واژه جنگ ترکیبی برای نخستین بار در پایان‌نامه ویلیام جی نمت در سال ۲۰۰۲ به‌کاربرده شد که در آن از تاکتیک‌های جنگ چریکی جنگجویان چچنی و استفاده آن‌ها از ابزار مدرن نظیر اینترنت و موبایل نام برده بود. در طی این پژوهش با مطالعه مقالات، سخنرانی ها، سایت‌ها، کتابها و.... به اهداف دشمن در جنگ ترکیبی پی برده و در پایان به نقش و اهمیت جنگ ترکیبی پرداخته‌ایم و دریافته‌ایم که امکان استفاده از این ظرفیت برعلیه ما توسط دشمنان، گروهای تروریستی و... وجود دارد، لذا باید با رصد و پایش و همچنین با اقدام فرهنگی تاب آوری و هشیار سازی را جهت پیشگیری و مقابله را بالا ببریم.

واژگان کلیدی: شبکه های اجتماعی، جنگ ترکیبی.

۱.مدرس دانشگاه افسری و تربیت پاسداری امام حسین (ع).

مقدمه

توسعه فناوری اطلاعات، ماهیت درگیری‌ها را با ایجاد لایه‌های پیچیده، نسبت به فضاهای نبرد سنتی تغییر داده است. دسترسی تقریباً جهانی به محیط مجازی فرصت‌های متعددی را برای انجام نبردهای آنلاین ایجاد کرده است که بر رویدادها در هر دو حوزه فیزیکی مانند سیستم‌های رایانه‌ای و در حوزه شناختی نگرش‌ها و باورهای افراد تأثیر می‌گذارد.

اخیراً شاهد بوده‌ایم که چگونه دولت‌ها و بازیگران غیردولتی از رویکردهای ترکیبی برای پیگیری اهداف سیاسی و نظامی خود استفاده می‌کنند و به طرز ماهرانه‌ای عملیات نظامی را با حملات سایبری، فشارهای دیپلماتیک، اقتصادی و کمپین‌های اطلاعاتی (تبلیغاتی) ترکیب می‌کنند. در طول دهه گذشته، رسانه‌های اجتماعی به‌سرعت به یکی از کانال‌های اصلی ارتباطی که امروزه مورد استفاده قرار می‌گیرد، تبدیل شده است. پلتفرم‌های ارتباط مجازی به بخشی جدایی‌ناپذیر از استراتژی جنگ تبدیل شده‌اند. درگیری‌های اخیر در لیبی، سوریه و اوکراین نشان داده است که رسانه‌های اجتماعی به‌طور گسترده برای هماهنگ کردن اقدامات، جمع‌آوری اطلاعات و مهم‌تر از همه برای تأثیرگذاری بر باورها و نگرش‌های مخاطبان هدف، حتی بسیج آن‌هابرای اقدام خاص استفاده می‌شوند.

با توجه به این وضعیت، نهادهای تحقیقاتی و امنیتی (مؤسسات و سیستم‌های امنیتی) وظیفه بررسی چگونگی استفاده بازیگران دولتی و غیردولتی از رسانه‌های اجتماعی را به‌عنوان ابزاری برای راهبردهای درگیری و جنگ ترکیبی بر عهده دارند. در گزارش به موضوعات زیر پرداخته خواهد شد.

۱. محیط جدید اطلاعاتی و نقش رسانه‌های اجتماعی

رشد سریع فناوری، محیط اطلاعاتی را که در آن زندگی می‌کنیم به‌طور چشمگیری تغییر داده است. فرصت‌های ارائه شده توسط فناوری اطلاعات به هر کسی اجازه می‌دهد تا هر زمان نیاز باشد از اطلاعات، تصاویر و ویدئوها استفاده کند و در فضای مجازی اشتراک‌گذاری داشته باشد.

این بستر به هر فردی این فرصت را می‌دهد که به یک بازیگر اطلاعات تبدیل شود و پیام‌ها را به‌طور بالقوه برای مخاطبان با تعداد و اندازه نامحدود در سراسر جهان توزیع کند. ماهیت ارتباطات فضای مجازی از الگوی «واحدی که صحبت می‌کنند و بسیاری گوش می‌دهند» به الگوی «بسیاری با بسیاری صحبت می‌کنند» تغییر کرده است یعنی تعامل بین شهروندانی که خودشان محتوا را ایجاد می‌کنند.

لذا دولت‌ها و رسانه‌های سنتی، دیگر مهم‌ترین بازیگران فضای اطلاعاتی نیستند. آن‌ها اکنون باید برای جایگاه خود در میان سایر بازیگران رقابت کنند و برای نیل به این هدف نیاز به تحلیل و شناخت این بستر اطلاعاتی است.

مشخصه محیط فضای مجازی:

دسترس‌پذیری

سرعت

ناشناس بودن

مبادله روزانه حجم بالایی از اطلاعات.

نامحدود بودن مرزهای جغرافیایی

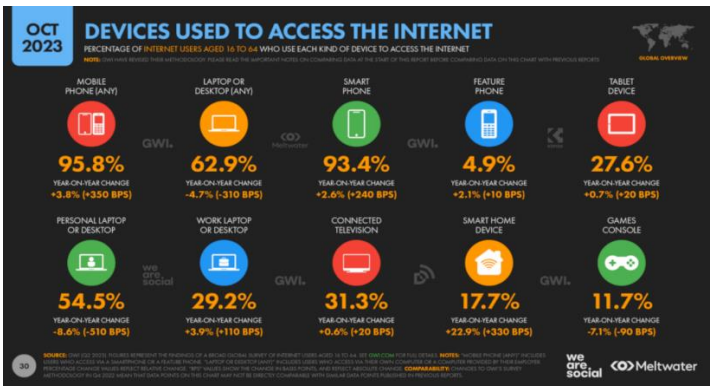
۱-۱.دسترس‌پذیری

جمع‌آوری و اشتراک‌گذاری اطلاعات با دستگاه‌های مدرنی مانند تلفن‌های هوشمند و دوربین که به هر کسی امکان فیلم‌برداری، ویرایش و اشتراک‌گذاری اطلاعات را تقریباً در لحظه انجام می‌دهد، آسان است.

با استناد بر گزارشی که توسط مؤسسه GWI انتشاریافته میزان دسترسی به اینترنت و فضای مجازی (شکل ۱) را نشان می‌دهد.

در شکل ۱ نشان می‌دهد که ۹۵% از کاربران اینترنت در گسترده سنی بین ۱۶ تا ٦٤ سال در بازه زمانی ۱۲ ماهه با گوشی هوشمند به اینترنت دسترسی داشته‌اند[۱] در حالیکه ۵٤/۵% از طریق لپ‌تاپ و کامپیوتر به اینترنت وصل شدند لذا می توان نتیجه گرفت که دسترسی جمعیت غالب جوامع امروزی به گوشی هوشمند به این معنی است که دسترسی به فضای مجازی آسان‌تر و قشر جوان به شدت تحت تأثیر قرار دارد.

علاوه بر این، این دستگاه‌ها نسبتاً ارزان هستند همچنین شبکه‌های تلفن همراه به‌خوبی توسعه یافته‌اند حتی مناطقی که سطح درآمد پایین دارند قادر به دسترسی به گوشی هوشمند هستند بنابراین موانع کمی برای استفاده از این فناوری برای به اشتراک‌گذاری اطلاعات وجود دارد.



شکل ۱

۱-۲. سرعت

رسانه‌های اجتماعی اطلاعات را به‌سرعت و با حجم بالا منتشر می‌کنند و با این قابلیت می توان حداکثر تأثیر را در مدت‌زمان بسیار کوتاهی به دست آورد.

محیط اطلاعاتی جدید یک محیط رقابتی است که در آن همه بازیگران برای شنیده شدن با هم رقابت می‌کنند. هر تردیدی باعث می‌شود دیگران داستان شما را برای شما تعریف کنند.

۱-۳. ناشناس بودن

ناشناس بودن در اینترنت به افراد اجازه می‌دهد تا آزادانه نظرات خود را بدون مسئولیت بیان کنند. کاربران ناشناس می‌توانند با ساختن محتوای بصری و متنی، انتشار اطلاعات و شایعات جعلی، ذهنیت مخاطبان را دستکاری کنند یا بدون مجازات به دیگر شرکت کنندگان در بحث‌های آنلاین حمله کنند.

۱-۴. مبادله روزانه حجم بالایی از اطلاعات

مقدار اطلاعاتی که در سراسر جهان از طریق پلتفرم‌های فضای مجازی به‌صورت روزانه ردوبدل می‌شود را می توان به رودخانه وسیعی که از شاخه‌های کوچک تشکیل شده مقایسه کرد.

کل داده‌های ایجاد شده، جمع‌آوری‌شده، کپی شده و مصرف‌شده [۲]در سطح جهانی به‌سرعت در حال افزایش بوده و در سال ۲۰۲۰ به ۶۴/۲ زتابایت[1]رسید. پیش‌بینی می‌شود، طی پنج سال آینده تا سال ۲۰۲۵، ایجاد داده‌های جهانی به بیش از ۱۸۰ زتابایت افزایش یابد. در سال ۲۰۲۰، میزان داده‌های ایجاد شده و تکرار شده به بالاترین حد خود رسید. این رشد بیشتر از انتظار قبلی بود که ناشی از افزایش تقاضا به دلیل همه‌گیری COVID-19 بود.

۱-۵. نامحدود بودن مرزها

قبل از ظهور رسانه‌های اجتماعی، یکی از نقش‌های رسانه‌های سنتی این بوده که به‌عنوان «بازیگر» عمل کنند یعنی موضوعات خاصی را پیش ببرند و بحث را شکل دهند. با ظهور رسانه‌های اجتماعی این تابع دیگر منحصر به آن‌ها نیست چون هر شخص یا گروهی می‌تواند این نقش را بازی کند به‌این‌ترتیب، بازیگرانی (مانند اقلیت‌ها، گروه‌های رادیکال و افراط‌گرایان) که هرگز فرصت بیان نظرات خود را از طریق رسانه‌های سنتی پیدا نمی‌کنند، می‌توانند از طریق رسانه‌های اجتماعی به مخاطبان گسترده‌ای دست یابند.

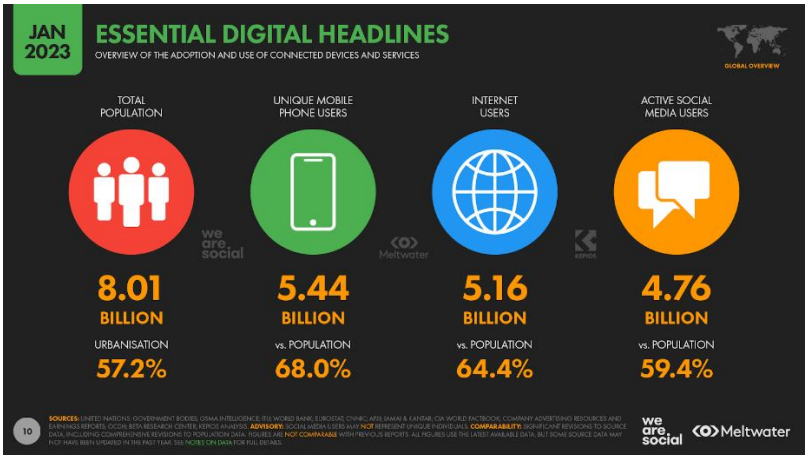
---

1. Zettabyte=1024 bit

۱-۵-۱. استفاده روزافزون اینترنت و فضای مجازی

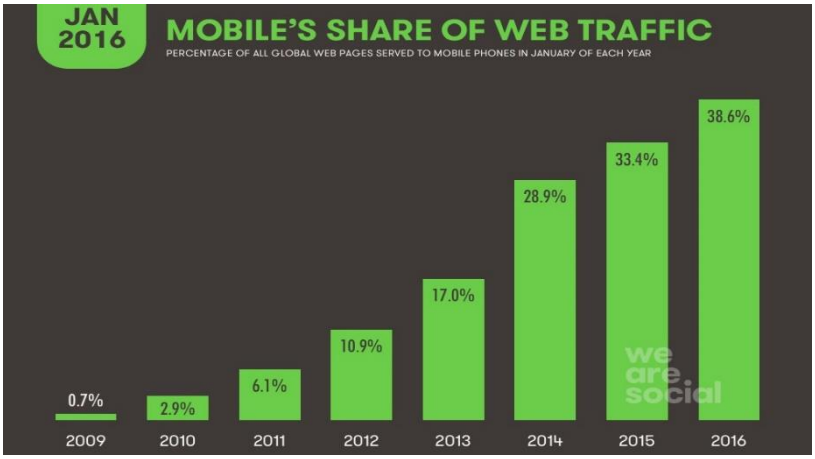
در ژانویه ۲۰۱٦ تقریباً نیمی (۳٫٤ میلیارد) از جمعیت جهان به‌طور فعال از اینترنت استفاده می‌کردند که تقریباً یک‌سوم (یا ۲٫۳ میلیارد) این جمعیت از سایت‌های شبکه‌های اجتماعی استفاده می‌کردند

این گزارش در حالی است که در سال ۲۰۲۳ هم‌اکنون ٤٫۷٦ میلیارد کاربر از جمعیت ۸ میلیارد نفری از رسانه‌های اجتماعی در سراسر جهان (شکل ۲) استفاده می‌کنند که معادل ٦۰ درصد از کل جمعیت جهانی است. [۳]



شکل ۲- میزان استفاده از رسانه‌های اجتماعی

شکل زیر (شکل ۳) که توسط WeAreSocial, StatCounter, Q1 2016 [٤] انتشار پیداکرده رشد استفاده از اینترنت (فضای مجازی) را نشان می‌دهد.



شکل ۳- نمودار رشد استفاده از اینترنت (فضای مجازی)

پلتفرم‌های رسانه‌های اجتماعی برای اهداف متفاوت استفاده می‌شوند. به‌عنوان مثال، فیس‌بوک (محبوب‌ترین سایت شبکه اجتماعی در سراسر جهان) عمدتاً برای شبکه‌سازی با دوستان و فامیل استفاده می‌شود.

سایت توییتر تبادل سریع پیام‌های کوتاه را فراهم می‌کند و پلتفرم‌های چت، امکان تبادل اطلاعات، تصاویر و ویدئوها را در یک شبکه فراهم می‌کند.

این پلتفرم‌ها فرصت‌های بی‌سابقه‌ای را برای افراد فراهم می‌کنند تا با دوستان خود و سایرین با علایق یا برنامه‌های مشابه ارتباط برقرار کنند و تجربیات/نظرات خود را به اشتراک بگذارند، فعالیت‌های دوستان خود را دنبال کنند و اطلاعات (ورزشی، فرهنگی، اخبار و غیره) را دریافت کنند[۵].

البته فضای مجازی نیز آثار مثبتی همچون بسیج مردم برای کمک به یکدیگر، جمع‌آوری بودجه برای اهداف اجتماعی، بررسی جنایات و ارائه کمک‌های بیشتر در بلایای انسانی به همراه داشته‌اند. همچنین این پلتفرم باعث افزایش سطح شفافیت در داخل دولت‌ها و افزایش توانایی مردم برای مشارکت در فرآیند تصمیم‌گیری، کشف دروغ‌ها و اطلاعات نادرست شده است.

بااین‌حال، همان محیطی که فرصت‌های بسیار خوبی را ارائه می‌دهد، می‌تواند آثار منفی نیز داشته باشد. گشودگی و تعاملی که اصول اساسی شبکه‌های اجتماعی را تشکیل می‌دهد می‌تواند ریشه آسیب پذیری های زیادی نیز باشد.

محیط مجازی یک محیط فاقد چهارچوب قانونی است که در آن ناشناس بودن فرصت‌های بیشتری را برای انتشار دیدگاه‌های افراطی، اطلاعات نادرست عمدی و ایجاد حقه‌ها بدون افشای شخص یا سازمان پشت ایجاد محتوا فراهم می‌کند. همانطور که دیوید استاپلز بیان می‌کند، سطح بالایی از ارتباطی که امروزه جمعیت‌ها دارند یک نقطه قوت است اما ارتباط فوری به این معنی است که اطلاعات نادرست و غلط نیز می‌تواند به‌سرعت گسترش یابد و منجر به وحشت شود[٦].

بنابراین رسانه‌های اجتماعی که از انبوهی از شبکه‌های مبتنی بر اعتماد تشکیل شده است، زمینه مساعدی را برای انتشار تبلیغات و اطلاعات نادرست و دستکاری ادراکات و باورهای ما فراهم می‌کند. به دلیل آثار بالقوه‌ای که فعالیت‌های رسانه‌های اجتماعی می‌توانند با هزینه یا تلاش اندک ایجادکنند، به ابزاری ضروری برای نبردهای جنگی تبدیل شده است که هم دولت‌ها و هم گروه‌های تروریستی از آن استفاده می‌کنند.

روش‌های مورد استفاده برای شکل دادن به عقاید مردم از زمان پیشرفت سریع این شکل از ارتباطات در دهه ۲۰۰۰ پیچیده‌تر می‌شوند.

۲. مفهوم جنگ هیبریدی

مفاهیمی مانند «غیرمتعارف»، «نامتقارن»، «نامنظم»، «ترکیبی» یا «جنگ نسل جدید» اغلب در بحث‌های سیاسی و دانشگاهی برای توصیف پیچیدگی و ویژگی‌های جنگ‌های مدرن که در آن بازیگران روش‌های مرسوم را با روش‌هایی ترکیب می‌کنند که خارج از درک سنتی ما از عملیات نظامی در استراتژی‌های جنگی آن‌ها قرار دارد را جنگ ترکیبی گویند.

اصطلاح "جنگ ترکیبی" اولین بار در سال ۲۰۰۲ در پایان‌نامه‌ای توسط William J. Nemeth که روشی را که شورشیان چچنی جنگ چریکی را با تاکتیک‌های نظامی مدرن و استفاده از موبایل و فناوری اینترنت ترکیب کردند، ظاهر شد. چچنی ها علاوه بر تاکتیک‌های عملیاتی بسیار انعطاف‌پذیر خود، از فعالیت‌های اطلاعاتی و عملیات روانی نیز علیه نیروهای روسی استفاده کردند[۷].

به منظور شناخت بیشتر جنگ هیبریدی نیاز به تشریح دکترین آن است.

تشریح دکترین جنگ هیبریدی[۸]:

جنگ هیبریدی به‌هیچ‌وجه به‌صورت رسمی اعلام نخواهد شد و گاهی عملیات نظامی با فعالیت گروه‌های شبه نظامی در زمان صلح آغاز می‌شود.

از درگیری‌های غیر تماسی بین گروه‌های جنگی باقابلیت مانور بالا استفاده می‌شود.

منابع نظامی و اقتصادی دشمن با حمله دقیق به زیرساخت‌های استراتژیک نظامی و غیرنظامی نابود می‌شود.

استفاده گسترده از سلاح‌های با دقت بالا و عملیات ویژه، سلاح‌های رباتیک و سلاح‌هایی که از اصول فیزیکی جدید استفاده می‌کنند (مانند سلاح‌های انرژی مستقیم مانند لیزر، تشعشعات موج کوتاه و غیره).

استفاده از ترکیبی از هوش مصنوعی، تجهیزات کنترل از راه دور، بمب‌ها یا مسلسل‌های با دقت بالا برای ترور مخالفان یا دشمنان(ترور دانشمند هسته‌ای ایران- فخری‌زاده).

- ❖ حمله همزمان به نیروها و تأسیسات دشمن درکل قلمرو،
- ❖ هک و نفوذ و غیرفعال سازی مراکز نظامی دشمن،
- ❖ انتشار اخبار دروغ و جعلی ،
- ❖ نبردهای همزمان در زمین، هوا، دریا و فضای اطلاعاتی،
- ❖ استفاده از روش های نامتقارن و غیرمستقیم .

علیرغم فقدان یک تعریف واحد، «جنگ ترکیبی» را می توان به‌عنوان شکلی از جنگ توصیف کرد که ترکیبی از روش‌ها اعم از متعارف و غیرمتعارف، نظامی و غیرنظامی، اقدامات آشکار و پنهان، سایبری و اطلاعاتی باهدف ایجاد سردرگمی و ابهام در ماهیت، منشأ و هدف ایجاد خواهند شد[۹].

می توان استدلال کرد که روش‌های غیرنظامی ازجمله عملیات اطلاعاتی همواره در زمان جنگ مورد استفاده قرارگرفته است. بااین‌حال، آنچه جنگ مدرن را بسیار متفاوت می‌کند، تأثیراتی است که اطلاعات می‌تواند بر توسعه درگیری ایجاد کند.

نقش حمله سایبری در جنگ هیبریدی

جنگ سایبری معمولاً شامل حمله به سیستم‌های رایانه‌ای است که زندگی روزمره و کسب‌وکار عامه مردم، زیرساخت‌های حیاتی، تراکنش‌های مالی، تأمین برق و غیره را مختل می‌کند.

همانطور که ریچارد کلارک، مشاور سابق کاخ سفید می‌نویسد، «حمله سایبری می‌تواند به این معنی باشد که سیستم‌ها حیاتی از کار می‌افتند و ما شاهد انفجار پالایشگاه‌های نفت، خروج قطارها از ریل، غیرفعال شدن ماهواره‌ها، کمبود مواد غذایی و موارد دیگر هستیم[۱۰].

رابرت بروس تحولات جنگ سایبری و به‌اصطلاح "جنگ شبکه" را که بیش از ۲۰ سال پیش به‌عنوان دو شکل نوظهور جنگ پیش‌بینی‌شده بود، مورد بحث قرار می‌دهد. جنگ سایبری به اختلال در سیستم‌های اطلاعاتی و ارتباطی اشاره دارد، درحالی‌که بازیگران در یک جنگ شبکه‌ای به‌طور آشکار و پنهان به دنبال "برهم زدن، آسیب رساندن یا اصلاح آنچه یک جمعیت هدف می‌داند یا فکر می‌کند در مورد جهان اطراف خود می‌داند" است[۱۱].

نگاهی به تاریخچه حملات سایبری در ایران

طی روزهای گذشته عجیب‌ترین حمله سایبری به تأسیسات کشور مردم را شوکه و متعجب کرد هرچند هنوز جزئیات دقیقی از این حمله آشکار نشده است. نهادهای مسئول در ابتدا این حمله سایبری را نپذیرفتند اما در نهایت اعلام شد که اختلال در سیستم سوخت‌رسانی کشور به‌طور سراسری نه به دلیل آسیب و کهنگی سیستم سوخت‌رسانی است و نه قرار است نرخ بنزین افزایش پیدا کند. روز چهارشنبه ۵ آبان سال ۱۴۰۲ یک حمله سایبری در کار بود که با مختل کردن جایگاه‌های سوخت سعی در مختل کردن خدمات عمومی بود.

در ذیل به پاره‌ای از حملات سایبری طی سالیان گذشته اشاره خواهد شد[۱۲]:

- حمله سایبری به تأسیسات هسته‌ای سال ۱۳۸۹،
- بازی‌های المپیک و استاکس‌نت؛ اولین حمله سایبری به تأسیسات کشور سال ۱۳۸۹،
- حمله با دو بدافزار به نام‌های Flame و Wiper به سیستم‌های نفتی و هسته‌ای سال ۱۳۹۱،

- ❖ آتش‌سوزی‌ها در پتروشیمی‌های ایران سال ۱۳۹۵،
- ❖ حمله سایبری به مرکز آمار سال ۱۳۹۵،
- ❖ حمله‌ای سایبری ماهواره پیام در سال ۱۳۹۷،
- ❖ حمله سایبری با نسل جدید استاکس‌نت سال ۱۳۹۷،
- ❖ حمله سایبری به سایت فرودگاه بین‌المللی مشهد سال ۱۳۹۷،
- ❖ ادعای حمله به زیرساخت‌های حوزه نفت و انرژی کشور در سال ۱۳۹۸،
- ❖ تکرار حمله به تأسیسات هسته‌ای و انتشار ویدیو از زندان اوین،
- ❖ حمله سایبری به شرکت راه‌آهن کشور سال ۱۴۰۰،

دشمن با افزایش حملات سایبری و مختل کردن خدمات عمومی در صدد نارضایتی مردم بوده.

"سلاح سازی" رسانه‌های اجتماعی:

نقش رسانه های اجتماعی در میدان‌ها جنگ:

از اولین "جنگ‌های اینترنتی" در کوزوو در سال ۱۹۹۹، درگیری بین حزب‌الله و اسرائیل و "بهار عربی" در شمال آفریقا و خاورمیانه تا درگیری‌های کنونی در سوریه و اوکراین، ما شاهدیم که چگونه فضای مجازی با شکل دادن به افکار عمومی، بسیج عمومی، هماهنگ کردن فعالیت‌های نظامی و جمع‌آوری اطلاعات برای اهداف استفاده شده‌اند. لذا فضای مجازی به‌طور فزاینده‌ای به "سلاح منتخب" برای بازیگران دولتی و غیردولتی تبدیل شده است.

جمع‌آوری اطلاعات، هدف‌گیری، اطلاع‌رسانی و نفوذ (جنگ روانی)، عملیات سایبری، دفاع و فرماندهی و کنترل. همه این فعالیت‌ها، صرف‌نظر از این‌که آثار آنلاین یا آفلاین داشته باشند، می‌توانند از طریق رسانه‌های شبکه‌های اجتماعی انجام شوند. این فعالیت‌ها پشتیبان یکدیگر هستند و اغلب می‌توانند در هماهنگی با فعالیت‌های فیزیکی روی زمین انجام شوند

رسانه‌های اجتماعی در میدان جنگ نقش مهمی دارند. زیرا رسانه‌های اجتماعی سلاح اصلی جنگ ترکیبی هستند و می‌توانند شایعات، تبلیغات، تحریکات و تأثیرات روانی را پخش کنند و از جهت دیگر رسانه‌های اجتماعی می‌توانند واقعیت‌های جنگ را به مردم نشان دهند و به آن‌ها کمک کنند تا تصمیمات اخلاقی بگیرند.

توماس الکجر نیسن[۱۳] شش راه را پیشنهاد می‌کند که می توان از رسانه‌های اجتماعی برای حمایت از عملیات در میدان جنگ استفاده کرد:

۱. هوش رسانه های اجتماعی(SOCMINT) ،
۲. استفاده از رسانه‌های اجتماعی برای شناسایی اهداف بالقوه،
۳. حملات سایبری،
۴. فرماندهی و کنترل،
۵. حفاظت از پلتفرم‌های فضای مجازی،
۶. شکل دادن به اخبار به منظور نفوذ.

هوش رسانه‌های اجتماعی(Social Media Intelligence (SOCMINT

SOCMINT به تکنیک‌ها، فناوری‌ها و ابزارهایی تعریف می‌شود که امکان جمع‌آوری و تجزیه‌وتحلیل اطلاعات از پلتفرم‌های رسانه‌های اجتماعی را فراهم می‌کند.

SOCMINT می‌تواند توسط بازیگران دولتی یا غیردولتی، مانند آژانس‌های اطلاعاتی خصوصی یا شرکت‌های بازاریابی، به‌منظور کسب دانش در مورد افراد، گروه‌ها، رویدادها یا هر تعداد هدف دیگر مورد استفاده قرار گیرد. [۱٤]

جست‌وجوی متمرکز و تجزیه‌وتحلیل اطلاعات از شبکه‌ها و پروفایل‌های افراد در فضای مجازی ازجمله محتوا و مکالمات می‌تواند به‌صورت آشکار یا پنهان انجام شود. چندین رویکرد برای تجزیه‌وتحلیل رسانه‌های اجتماعی برای جمع‌آوری اطلاعات وجود دارد (مانند پروفایل، بیوگرافی، احساسات، جغرافیا، محتوا، رفتار کاربران و هر چیز دیگری) لذا تجزیه‌وتحلیل همه این اشکال می‌توانند به تجزیه‌وتحلیل مخاطبان (هدف) کمک کنند و از جنگ روانی یا انتخاب اهداف برای عملیات آنلاین و آفلاین پشتیبانی کنند.

اساساً رسانه‌های اجتماعی امکان دریافت اطلاعات دقیق در مورد شبکه‌ها، بازیگران و ارتباطات مرتبط را فراهم می‌آورند و به‌این‌ترتیب به هر گروهی کمک می‌کند تا بدون حضور فیزیکی، درک بهتری از محیط اطلاعاتی و وضعیت هر گروه هدف داشته باشد. اگر تجزیه‌وتحلیل به‌طور مداوم صورت گیرد رسانه‌های اجتماعی می‌توانند منبع مفیدی برای آگاهی از موقعیت و حتی برای شناسایی "سیگنال‌های" یک بحران در آینده باشند.

استفاده از رسانه‌های اجتماعی برای شناسایی اهداف بالقوه

استفاده از Social Media برای شناسایی اهداف بالقوه برای اقدامات نظامی در حوزه فیزیکی (بر اساس برچسب جغرافیایی، مکالمات یا برحسب لوکیشن حساب‌ها/اکانت‌های کاربران در رسانه‌های اجتماعی) و همچنین برای حمله به حساب‌های رسانه‌های اجتماعی (مخالفان) از طریق هک یا تخریب کاربران صورت خواهد گرفت.

به‌عنوان مثال، نقشه‌های گوگل و تلفن‌های همراه در لیبی برای نقشه‌برداری از مواضع رژیم استفاده شد که سپس به ناتو منتقل شد و ناتو از این اطلاعات برای شناسایی اهداف و درگیری با آن‌هابا استفاده از نیروی هوایی استفاده کرد.

نمونه دیگر حمله به ساختمان مقر داعش، توسط نیروی هوایی آمریکا، تنها بیست و دو ساعت پس از شروع ردیابی پست‌های داعش در شبکه‌های اجتماعی بود[۱۵].

حملات سایبری

عملیات سایبری می‌تواند تهاجمی یا تدافعی باشد نمونه‌ای از این عملیات شامل هدف قرار دادن پلتفرم‌های رسانه‌های اجتماعی، حک کرد رمز عبور اکانت‌ها، غیرقابل استفاده کردن یک وب‌سایت و غیره باشد.

بااین‌حال اکثر عملیات سایبری بر روی رسانه‌های اجتماعی ماهیت تهاجمی دارند. آن‌ها می‌توانند شامل اقداماتی مانند حملات (DDos) به وب‌سایت‌ها، هک رمز عبور برای دسترسی و افشای محتوای حساب‌ها، ایمیل‌ها یا تلفن‌های همراه، تغییر محتوا در حساب‌های رسانه‌های اجتماعی یا نفوذ به پایگاه‌های اطلاعاتی برای جمع‌آوری اطلاعات باشند.

تمام این فعالیت‌ها باهدف جلوگیری از استفاده دیگر بازیگران از پلتفرم‌های رسانه‌های اجتماعی برای برقراری ارتباط، هماهنگی اقدامات، دسترسی به اطلاعات یا توزیع پیام‌ها حداقل به‌طور موقت انجام می‌شوند.

فرماندهی و کنترل

استفاده از رسانه‌های اجتماعی برای فرماندهی و کنترل بازیگران غیردولتی مانند گروه‌های شورشی مهم است، به‌ویژه اگر این گروه‌ها فاقد ساختار رسمی باشند یا در مناطق جغرافیایی وسیعی پراکنده باشند.

رسانه‌های اجتماعی می‌توانند ابزار ارتباطی و راهی برای هماهنگی فعالیت‌های آن‌ها فراهم کنند. بااین‌حال، استفاده از رسانه‌های اجتماعی فعالیت‌های گروه‌های شورشی را در معرض دید سرویس های اطلاعاتی قرار می‌دهد.

چنین ترتیبات فرماندهی و کنترلی «باز» مبتنی بر رسانه‌های اجتماعی، حمله به شبکه‌های بازیگران غیردولتی را برای نیروهای مسلح متعارف دشوار می‌کند زیرا هیچ شبکه متمرکز، گره یا هدف فیزیکی برای حمله وجود ندارد و ازآنجایی‌که زیرساخت‌ها و پلتفرم‌ها نظامی نیستند، هرگونه حمله با مسائل حقوقی مختلفی همراه است.

رسانه‌های اجتماعی همچنین می‌توانند برای تاکتیک‌های «ازدحام» استفاده شوند یعنی توزیع اطلاعات برای بسیج و هماهنگ کردن بازیگران غیردولتی با منافع مشترک برای تعامل با یک هدف خاص.

به گزارش ایسنا، به نقل از خبرگزاری فرانسه، حکومت‌ها در سراسر شمال آفریقا و خاورمیانه در حالی غافلگیر شدند که شور قیام‌های مردمی با سرعت اینترنت و از طریق فیسبوک، یوتیوب و توئیتر گسترش پیدا کرد.

سامی بن غربی، یک فعال معترض سابق تونسی که اداره‌کننده یک وبلاگ بوده گفت: بلاگ‌ها و شبکه‌های اجتماعی عامل جرقه نبودند اما آن‌ها از جنبش‌های اجتماعی حمایت کردند. آن‌ها سلاح ارتباطی عالی بودند[۱۶].

حفاظت از پلتفرم‌های فضای مجازی

حفاظت از پلتفرم‌های رسانه‌های اجتماعی، سایت‌ها، پروفایل‌ها در سطح فنی یا سیستمی برای دولت‌ها امری اساسی است.

زیرا گروه‌های خاطی و سازمان‌های تروریستی می‌تواند با استفاده از رمزکننده، نرم‌افزار رمزگذاری، ضد ردیابی یا پنهان‌کننده IP در شبکه اینترنت عملیات خود را هماهنگی و مدیریت کنند.

با توجه به این شرایط، جای تعجب نیست که سازمان‌های تروریستی عمدتاً از پلتفرم‌های چت رمزگذاری شده برای ارتباط بین حامیان خود استفاده می‌کنند. به‌عنوان مثال، مشخص شده است که پلی‌استیشن یکی از چالش برانگیزترین پلتفرم‌های بازی برای ردیابی سرویس‌های اجرای قانون است.

به عنوان یک نمونه، حمله گروه داعش (هشت تروریست، تاریخ ۲۲ مارس ۲۰۱۶) که مسئول یورش به بروکسل بودند. وزیر امور داخلی فدرال بلژیک، جان جامبون، صریحاً گفته است که PS4 توسط عوامل داعش برای برقراری ارتباط استفاده می‌شود و دلیل انتخاب این پلتفرم این است که نظارت بر آن بسیار سخت است و پیگیری پلی‌استیشن ٤ حتی از واتس اپ دشوارتر است[۱۷].

علاوه بر این، داعش به اعضای خود در مورد خطرات ناشی از نادیده گرفتن امنیت سایبری هشدار داده است و در دسامبر ۲۰۱٤ فرمانی صادر کرد که جنگجویان خود را از فعال کردن عملکرد برچسب‌گذاری جغرافیایی توییتر منع کرد. و پیشنهاداتی در مورد چگونگی تضمین امنیت عملیاتی در

محیط مجازی ارائه می‌کند داعش همچنین یک دفترچه راهنمای آنلاین و راهنمای حفظ حریم خصوصی ایجاد کرده است که پیشنهاداتی را در مورد چگونگی تضمین امنیت عملیاتی در محیط مجازی ارائه می دهد[۱۸].

شکل دادن به اخبار و نفوذ

به انتشار اطلاعات هدفدار برای تأثیرگذاری بر ارزش‌ها، سیستم اعتقادی، ادراکات، احساسات، انگیزه، استدلال و رفتار مخاطب اشاره دارد.

یکی از اهداف استفاده از Social Media در حوزه شناختی بر شکل دادن، نفوذ، دستکاری، افشا و ترویج اخبار و اطلاعات جهت‌دار به‌منظور فریب، بازدارندگی، بسیج کردن و متقاعد کردن جامعه هدف است[۱۹].

روش‌های نفوذ مورد استفاده در رسانه‌های اجتماعی می‌تواند آشکار باشد (مانند ایجاد حساب‌های رسمی، کانال‌ها و وب‌سایت‌ها به‌منظور انتشار نظرات و افکار رهبران و غیره یا مخفیانه (مانند هویت‌های جعلی، بات‌نت‌ها و ترولینگ) باشد.

نظر دکتر ربکا گولزبی[۲۰]در مورد مقاصد مختلف تعامل با رسانه‌های اجتماعی در مورد "حملات سایبری اجتماعی" غیرسازمانی و سازمانی:

«مجموعه اقدامات عمدی و سازمانی برای انتشار شایعات، فریب‌کاری‌ها و پیام‌ها به‌منظور دستکاری در محیط مجازی باهدف افزایش ترس و وحشت به‌گونه‌ای که ردیابی سازمان‌دهندگان و عاملان حملات سایبری پنهان ماند».

دکتر گولزبی موردی را در آسام هند در ژوئیه ۲۰۱۲ توصیف می‌کند که توزیع تصاویر جعلی و پیام‌های متنی در مورد حملات علیه جمعیت مسلمان منجر به مهاجرت دسته‌جمعی شد.

نقش رسانه‌های معاند در جنگ ترکیبی

حسن هانی زاده، کارشناس ارشد مسائل بین‌الملل در گفتگو با دیار آفتاب با بیان این که اغتشاشات اخیر برآیند یک ائتلاف جهانی برای تحمیل جنگ ترکیبی علیه ایران بود گفت: گزارش‌ها نشان می‌دهد که بیش از ۴۰ کشور در سراسر جهان در این جنگ ترکیبی و شناختی و جنگ نرم علیه ایران به انواع گوناگون شرکت داشته‌اند.

این کارشناس مسائل بین‌الملل تصریح کرد: [۲۱] عربستان در فاز رسانه‌ای تأمین‌کننده مالی شبکه‌های رسانه‌ای تروریستی، صهیونیستی و سعودی بود و به‌عنوان تأمین‌کننده هزینه‌های مالی رسانه‌های معاند سالانه ده میلیارد دلار هزینه می‌کند.

مهناز حسینی خبرنگار صداوسیما [۲۲] در مورد رسانه‌های فارسی‌زبان خارج‌نشین گفت: یکی از شبکه‌های ماهواره‌ای شبکه اینترنشنال است؛ دو سالی می‌شود که این شبکه ایجاد شده و پشتوانه آن عربستان سعودی است و منابع مالی‌اش را اسرائیل تأمین می‌کند. اسرائیل در هر سال حدود ۵۰ میلیون دلار پول برای این شبکه اختصاص داده است. هدف آن هم تمرکز بر روی قشرهای خاصی است و از طریق جنگ‌های رسانه‌ای شناختی تلاش می‌کند بر روی احساسات مردم کار کند و آنان را تشویق به کاری کند که دلخواهش است.

جنگ ترکیبی آمریکا علیه ایران

در باب مولفه‌های جنگ ترکیبی ایالات متحده علیه ایران محسوس‌ترین بُعد، اقتصادی است. وقتی از جنگ اقتصادی صحبت می‌کنیم راجع به طیف متنوعی از تهدیدات و منازعات صحبت می‌کنیم که تحریم یکی از آن‌ها است. غیر از تحریم، آمریکایی‌ها به دلیل توان اقتصادی و به دلیل انحصار منابع در تولید، باز جمهوری اسلامی را محدود می‌کنند. غیر از بحث منابع، بحث نهادهای بین‌المللی هم مطرح است. مقوله دیگر بحث شکل دادن ائتلاف‌ها و اتحادهای اقتصادی است.

جنگ‌های سایبری نیز یکی دیگر از مهم‌ترین محورهای جنگ هیبریدی ایالت متحده علیه ایران است. وقتی از جنگ سایبری صحبت می‌کنیم، با طیف متنوعی از موضوعات مواجه هستیم.

جنگ‌های فرهنگی و تبلیغاتی هم بخش مهمی از جنگ‌های ترکیبی است. همچنین در دنیای امروز نهادی به نام سازمان رسانه جهانی شکل گرفته که به طور تقریبی تمام رسانه‌ها به آن متصل هستند. این سازمان به طور دقیق سازمان اطلاعاتی و نظامی است. در تمام فضاهایی مثل گوگل، ظرفیت‌هایی ایجاد شده که آرزوی دیرین دولت‌ها را در ثبت اطلاعات کشورهای مختلف بر عهده گرفته است[۲۳].

نقش جنگ ترکیبی در اعتراضات ایران

مفهوم جنگ و الگوهای آن روزبه‌روز در حال تغییر و تطور است. در این بین و با ظهور جوامع پیچیده شبکه‌ای به‌عنوان بستر مدرن برای زیست قدرت، الگوهای جنگ مدرن نیز در حال ظهور هستند. جنگ ترکیبی به‌عنوان یکی از الگوهای مدرن جنگ در این قالب قابلیت پردازش دارد. جمهوری اسلامی ایران همواره هدف انواع تهاجم‌های غرب بوده و هست. ازاین‌رو واکاوی مدل‌های جنگ علیه جمهوری اسلامی ایران از اهمیت زیادی برخوردار است در این بین یکی از ابزارهای غرب با استفاده از ابزارهای رسانه‌ای ضمن تهاجم به اصول، ارزش‌ها و تضعیف باورهای اجتماعی حریف و جایگزینی روایت‌های جعلی بجای واقعیات و همچنین انتشار اخبار دروغین و شایعه پراکنی در اغتشاشات بود.

کمال خرازی مشاور وقت رهبر انقلاب گفت: آنچه در ایران رخ داد یک جنگ هیبریدی بود که در آن جنگ سیستم خبری و عملیات تروریستی و هم دستگاه‌های سیاسی کشورها و اطلاعاتی کشورها در

آن درگیر بودند و این طراحی و آتش را برافروزند که متأسفانه فوت مرحومه امینی این بهانه را به دست آن‌ها داد و چنین اغتشاشی را سامان داد.

رسانه‌های معاند فارسی‌زبان خارج کشور بالأخص عربستان سعودی با انتخاب گزینشی خبرها و با حمایت اتاق فرماندهی جنگ روانی آمریکا و اسرائیل تلاش کردند با گسترده نمایی اعتراضات و نقاط ضعف تلاش کردند تا نارضایتی عمومی را افزایش دهند و با تشدید شکاف‌های اجتماعی بی‌اعتبار کردن نمادهای قدرت را در سرلوحه کار خود قرار دهند و از گروه‌های تجزیه‌طلب، در بستر اعتراضات حمایت کنند و امنیت ملی را تهدید و خدشه‌دار کنند تا جایی که به گفته روزنامه «رأی الیوم» نسخه ۲۰۲۲ عملیات «آژاکس» که برای براندازی دولت مصدق استفاده شد بار دیگر در ایران اجرا شود.

این جنگ ترکیبی بر پایه جنگ شناختی و عملیات روانی دشمن استوار بود و سخنان هشدار آمیز فرمانده‌کل سپاه پاسداران انقلاب اسلامی[۲۴] در ۲۵ مهر حاکی از این مسأله بود. سردار سلامی اذعان کرد به رژیم آل سعود هشدار می‌دهم که مراقب رفتارتان باشید و این رسانه‌ها را کنترل کنید وگرنه دود آن به چشم خودتان خواهد رفت.

ترولینگ اینترنت

سازماندهی فعالیت‌ها با استفاده از هویت‌های جعلی در اینترنت و رسانه‌های اجتماعی به‌منظور دستیابی به تأثیرات خاص چیز جدیدی نیست. بااین‌حال، درگیری روسی و اوکراین باعث تشدید بحث در مورد چگونگی استفاده از ترول به‌عنوان ابزاری برای دستکاری افکار مردم با گسترش تبلیغات و شایعات و تحریف اطلاعات شد.

ترولینگ از اواخر دهه ۱۹۸۰ و اوایل دهه ۱۹۹۰ مطرح شد که در آن زمان یک رفتار اجتماعی جدید بود. ترول ها معمولاً سعی می‌کردند با طرح سؤالات تحریک‌آمیز یا ارسال دیدگاه‌های افراطی در مورد موضوعات بحث‌برانگیز، اختلافات پنهان بین اعضای جامعه را آشکار کنند.

ترول [۲۵] (به انگلیسی: Troll) یا اوباش مجازی، در گفتمان اینترنتی به افرادی گفته می‌شود که با رفتار مخرب در فضای وب به دنبال جلب نظر کاربران، ایجاد تشنج و بیان مطالب تحریک‌کننده و توهین‌آمیز هستند.

نقش رسانه‌های اجتماعی در فعالیت‌های اطلاعاتی روسیه

عملیات نظامی روسیه علیه اوکراین که منجر به الحاق کریمه در مارس ۲۰۱۴ و جنگ مداوم در شرق اوکراین شد، نمایشی از رویکرد جنگی نسل جدید روسیه است که در آن از ابزارهای نظامی سنتی در کنار ترکیبی از جنگ اطلاعاتی، حملات سایبری و دیپلماسی استفاده شد.

استفاده از فضای مجازی چه در جنبه فنی و چه در جنبه‌های محتوایی، نشان می‌دهد که چگونه رهبران روسیه با محیط شبکه‌های اجتماعی (Social Media) سازگار شده‌اند و تأکید زیادی بر اطلاعات و کنترل اطلاعات دارند[۲٦].

دکترین نظامی روسیه از دسامبر ۲۰۱٤ بر تهدیدهای ژئوپلیتیکی گسترده‌ای که روسیه در حال حاضر با آن روبه رو است و همچنین روش‌های جدیدی که غرب علیه روسیه استفاده می‌کند، تأکید می‌کند. این تهدیدات، روسیه را وادار به واکنش و ایجاد راهبرد جدید واکنشی کرده است که متشکل از اقدامات نظامی و غیرنظامی است و ترکیبی از روش جدید و غیر سنتی را در بر می گیرد[۲۷].

نتیجه‌گیری

توسعه فناوری، عرصه جنگ و درگیری را تحت تأثیر قرار داده است زیرا مسلسل‌ها و تانک‌ها اکنون با سلاح‌هایی جایگزین شده‌اند (جنگ رسانه ای) که دیده نمی‌شوند.

اگرچه به نظر نمی‌رسد که رسانه‌های اجتماعی به‌اندازه رسانه‌های جریان اصلی مؤثر باشند اما نقش رسانه‌های اجتماعی از نظر جریان اطلاعات بی‌صدا است.

رسانه‌های اجتماعی این قدرت را دارند که محتوا را با حجم و سرعتی بالا منتشر کنند و در مدت‌زمان کوتاهی به‌عنوان ابزار مؤثر جنگ ترکیبی برای تأثیرگذاری و تغییر نگرش عقاید و رفتار مردم برای تحقق اهداف سیاسی یا نظامی خاص مورد استفاده قرار می‌گیرند.

در فضای مجازی کاربر با ناشناس بودن می‌تواند آزادانه و بدون ترس از مسئولیت و بدون هیچ‌گونه مرز جغرافیایی یا محتوایی، نظر خود را بیان کند. ازاین‌رو، دولت و همچنین بازیگران غیردولتی استفاده گسترده از رسانه‌های اجتماعی را برای تبلیغ ایدئولوژی خود برای تأثیرگذاری بر افکار و عقاید مخاطبان آغاز کردند.

رسانه‌های اجتماعی می‌توانند توسط گروه‌های شبه‌نظامی و تروریستی برای تحقق اهداف خاص خود مورد استفاده قرار گیرند.

لذا فضای مجازی با قابلیت‌هایی ازجمله انتقال محتوا با سرعت و حجم نامحدود، پنهان‌کاری، محرمانگی، غیرقابل کنترل و نظارت بودن، ناشناس بودن، انتشار آزادانه اطلاعات و... به‌عنوان ابزاری مناسب نقش بسزایی در جنگ‌های ترکیبی دارند که هم توسط دولت‌ها و هم توسط گروه‌ها مورد استفاده قرار می‌گیرند بنابراین این شعار را باید آویزه گوش کرد که جنگ آینده، جنگ رسانه است و جنگ رسانه در ترکیب با حملاتی همچون انفجار پالایشگاه‌های نفت، خروج قطارها از ریل، غیرفعال شدن ماهواره‌ها، کمبود مواد غذایی و از دست رفتن خدمات عمومی در کنار جنگ مسلحانه در میدان نبرد درمجموع دلالت بر جنگ هیبریدی دارند.

منابع و مراجع

1. https://datareportal.com/reports/digital-2023-global-digital-overview.
2. https://www.statista.com/statistics/871513/worldwide-data-created.
3. https://datareportal.com/reports/digital-2023-global-digital-overview.
4. WeAreSocial, StatCounter, Q1 2016.
5. 'Social Networking Motivations', Global Web Index Insight Report 2015, http://www.globalwebindex.net/blog/top 10-reasons-for-using-social-media.
6. David Stupples, 'The next big war will be digital and we are not ready for it', The Conversation, November 26, 2015, https://theconversation.com/the-next-war-will-be-an information-war-and-were-not-ready-for-it-51218.
7. Andras Racz, 'Russia's Hybrid War in Ukraine: Breaking Enemy's Ability to Resist', FIIA Report 43, 2015, p.28, http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ ukraine/.
8. Jānis Bērziņš, 'Russia's new generation warfare in Ukraine: Implications for Latvian defense policy', Policy Paper No 2, 2014, p.4, http://www.naa.mil.lv/~/media/NAA/AZPC/ Publikacijas/PP%2002-2014.ashx.
9. Jan Joel Andersson 'Hybrid operations: lessons from the past', EUISS, October 2015, http://www.iss.europa.eu/ uploads/media/Brief_33_Hybrid_operations.pdf.
10. Richard A. Clarke & Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It, New York: HarperCollins, 2011Robert Brose, 'Cyberwar, Netwar and the Future of Cyberdefence', Office of Director of National Intelligence. United States of America, 11 June 2015, http://www.dni.gov/index.php/ newsroom/ic-in-the-news/211-ic-n-the-news-2015/1205-cyber war,-netwar,-and-the-future-of-cyberdefense.
11. Robert Brose, 'Cyberwar, Netwar and the Future of Cyberdefence', Office of Director of National Intelligence. United States of America, 11 June 2015, http: //www.dni.gov/index.php/ newsroom/ic-in-the-news/211-ic-n-the-news-2015/1205-cyber war,-netwar,-and-the-future-of-cyberdefense.

۱۲. نگاهی به تاریخچه حملات سایبری تایید و تکذیب شده در ایران(digiato.com).

13. Nissen, The Weaponization of Social Media, p. 72
14. Everything About Social Media Intelligence (SOCMINT) and Investigations – Maltego
15. Walbert Castillo, 'Air Force Intel Uses ISIS 'moron' Post to Track Fighters', 5 June 2015, http://edition.cnn. com/2015/06/05/politics/air-force-isis-moron-twitter/.

۱۶. بهار عربی؛ اولین انقلاب اسمارتفونی - ایسنا(isna.ir)

17. https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/?sh=59813ae7055.
18. 'Islamic State issues anti-hacking guidelines after Anonymous threats', 17 November, 2015, http://www.telegraph.co.uk/technology/internetsecurity/12001420/Islamic-State-issues-anti-hacking-guidelinesafter-Anonymous-threats.html
19. Nissen, The Weaponization of Social Media.
20. Rebecca Goolsby. 'On Cybersecurity, Crowdsourcing and Social Cyber-Attack.' Washington: Wilson Center. U.S. Office of Naval Research, 2013., https://www.wilsoncenter.org/sites/ default/files/127219170-On-Cybersecurity-Crowdsourcing Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.

۲۱. رسانه‌های معاند در جنگ ترکیبی چه نقشی دارند؟(dana.ir)

۲۲. جنگ‌های رسانه‌ای و روش‌های مقابله‌ای با آن(vasael.ir)

۲۳. ابعاد جنگ هیبریدی؛ از دیپلماسی هسته‌ای تا عملیات نفوذ - ایرنا(irna.ir)

۲۴. چیستی راهکارهای ایران در جنگ هیبریدی(basirat.ir)

۲۵. ترول اینترنتی - ویکی‌پدیا، دانشنامه آزاد(wikipedia.org)

26. Margarita Jaitner, Dr Peter A. Mattsson, 'Russian Information Warfare of 2014', 7th International Conference on Cyber Conflict: Architectures in Cyberspace, NATO CCD COE Publication, 2015, p. 48. https://ccdcoe.org/cycon/2015/ proceedings/03_jaitner_mattsson.pdf.
27. Jolanta Darczewska, 'The Devil is in the Details. Information Warfare in the Light of Russia's Military Doctrine', Point of View, Centre for Eastern Studies, Warsaw, May 2015, p. 9, http://www.osw.waw.pl/sites/default/files/pw_50_ang_thedevil-is-in_net.pdf.