فصلنامه مطالعات جنگ
سال دوم، شماره چهارم، بهار ۱۳۹۹
مقالهٔ سوم از صفحه ۵۸ تا ۷۱

کاربردهای جنگ رسانه‌های اجتماعی در عملیات نظامی

ندا انعامی[۱]، محمدرضا کریمی قهرودی[۲]

دریافت مقاله: ۹۹/۰۱/۰۸ **پذیرش مقاله: ۹۹/۰۲/۲۸**

چکیده

رشد و توسعه فضای سایبر و پیشرفت‌های فناوری اطلاعات، ماهیت درگیری‌ها را با ایجاد پیچیدگی بیشتر متحول نموده است. دسترسی تقریباً جهانی به محیط مجازی، موقعیت آن را فراهم نموده است تا نبردهایی به‌صورت آنلاین هدایت گردند که هر دو قلمرو فیزیکی، نظیر سیستم‌های رایانه‌ای و قلمرو شناختی یعنی نگرش‌ها و عقاید افراد را تحت تأثیر قرار دهند. که اولی نمایانگر جنگ سایبری و دومی مطرح کننده حوزه نوینی از جنگ به نام جنگ رسانه‌های اجتماعی است. از سوی دیگر جنگ ترکیبی رویکرد نوینی به جنگ است که از ترکیب جنگ‌های کلاسیک و نبردهای سایبری و اطلاعاتی تشکیل می‌شود. مرز بین جنگ سایبری و جنگ اطلاعات با ظهور رسانه‌های اجتماعی در حال محو شدن است. آنچه مسلم است با به‌کارگیری رسانه‌های اجتماعی به‌عنوان ابزاری در جنگ می‌توان هر دو قلمرو فیزیکی و شناختی را به‌طور توأمان تحت تأثیر قرار داده و به نتایج مهم‌تری دست یافت. در این مقاله به نحوه استفاده از رسانه‌های اجتماعی در جنگ ترکیبی و نحوه مسلح سازی شبکه‌های اجتماعی خواهیم پرداخت و شیوه‌های مختلف به‌کارگیری رسانه‌های اجتماعی در عملیات نظامی از جمله جمع‌آوری اطلاعات، هدف‌یابی، تلقین کردن و جنگ روانی، عملیات سایبری، دفاع کردن و فرماندهی و کنترل را تشریح خواهیم نمود.

واژگان کلیدی: **رسانه اجتماعی، جنگ روانی، عملیات سایبری**

۱ - پژوهشگر حوزه سایبر
۲ - عضو هیئت‌علمی دانشگاه صنعتی مالک اشتر

مقدمه

رسانه‌های اجتماعی با ویژگی‌های خاص خود چون دسترسی آسان، سرعت در انتشار اطلاعات و حجم بالای تبادل اطلاعات، عدم وابستگی جغرافیایی و تعاملی کردن رسانه‌های ارتباط‌جمعی از طریق ایجاد قابلیت به اشتراک‌گذاری نظرات و تجارب افراد، مزایای بسیاری را برای انسان امروزی به ارمغان آورده‌اند. از جمله این مزایا کمک به همنوعان، رسیدگی به جرائم، کمک در عملیات امداد و نجات در طول فجایع انسانی، شفافیت در دولت و اداره کشور و همچنین گفتگوی میان گروه‌های مختلف اجتماعی، سیاسی و می‌باشد.

بااین‌وجود همین ویژگی‌های خاص رسانه‌های اجتماعی نظیر گمنامی کاربران و حجم بالای اطلاعاتی که روزانه در جهان ردوبدل می‌گردد، چالش‌هایی نظیر عدم امکان تشخیص صحت‌وسقم اطلاعات، انتشار اخبار و شایعات دروغ، تبلیغات منفی و دست‌کاری ادراکات و باورهای افراد را مطرح می‌کنند که این تهدیدات ممکن است بر جنگ‌ها تأثیرگذار باشند. این تأثیرگذاری تا حدی است که به اعتقاد برخی از صاحب‌نظران، رسانه‌های اجتماعی در حال متحول نمودن شیوه و دلایل جنگ‌ها هستند.

از سوی دیگر جنگ ترکیبی رویکرد نوینی به جنگ است که از ترکیب جنگ‌های کلاسیک و نبردهای سایبری و اطلاعاتی تشکیل می‌شود. در نبود یک تعریف یکپارچه، «جنگ‌های ترکیبی» را می‌توان به‌عنوان نوعی از جنگ معرفی کرد که شامل ترکیبی از روش‌های متعارف و غیرمتعارف، نظامی و غیرنظامی، اقدامات آشکار و پنهانی شامل جنگ سایبری و اطلاعات با هدف ایجاد سردرگمی و ابهام در ماهیت، منشأ و هدف این اقدامات است.

مرز بین جنگ سایبری و جنگ اطلاعات با ظهور رسانه‌های اجتماعی در حال محو شدن است. فعالیت‌های فضای سایبری نه‌تنها برای مختل کردن سیستم‌های اطلاعاتی فیزیکی بکار می‌روند بلکه بر نگرش و رفتار تأثیر می‌گذارند تا به اهداف نظامی یا سیاسی معین دست یابند. آنچه مسلم است با به‌کارگیری رسانه‌های اجتماعی به‌عنوان ابزاری در جنگ می‌توان هر دو قلمرو فیزیکی و شناختی را به‌طور توأمان تحت تأثیر قرار داده و به نتایج مهم‌تری دست یافت. می‌توان استدلال کرد که روش‌های غیرنظامی، از جمله عملیات اطلاعاتی، همیشه در زمان جنگ استفاده شده است. بااین‌حال، آنچه جنگ مدرن را این‌قدر متفاوت می‌کند، اثراتی است که اطلاعات می‌تواند در جهت توسعه درگیری ایجاد کند، زیرا درک مخاطبان از نتیجه

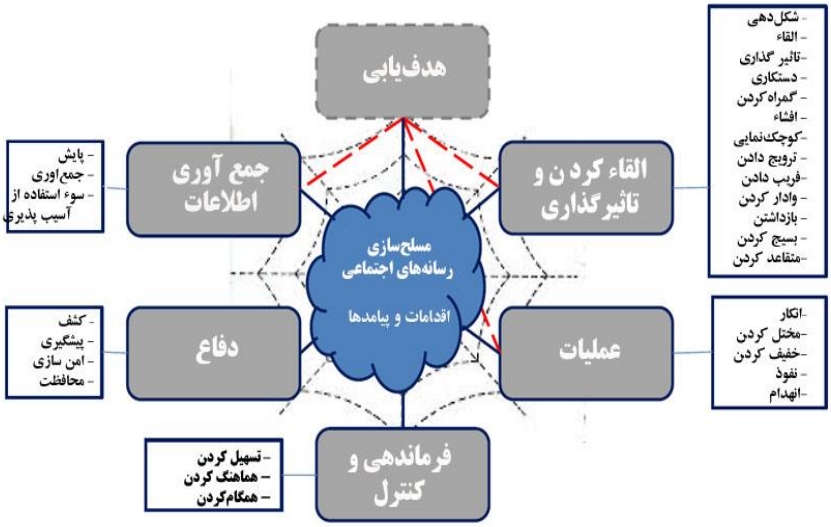
درگیری، مهم‌تر از حقایق کنونی روی زمین است. توانایی فناورانه ای کـه مـا در حـال حاضـر برای تعقیب اقدامات، تقریباً بدون محدودیت‌های جغرافیایی در اختیار داریم، باعـث مـی‌شـود مشارکت مخاطبان جهانی در درگیری حتی مهم‌تر از قبل گـردد. مخاطبـان داخلـی، پراکنـده و خارجی هم‌اکنون می‌توانند با وقایع به‌صورت بلادرنگ ارتباط برقـرار کننـد، زیـرا آن‌هـا منـابع خبری آنلاین را دنبال کرده و از طریق رسانه‌های اجتماعی متصل می‌شوند. هنگام بحث درباره نقش رسانه‌های اجتماعی، اغلب به‌عنـوان بخشـی از فضـای سـایبری بـه آن اشـاره مـی‌شـود، بااین‌وجود تمایز قائل شدن بین اینکه از رسانه‌های اجتماعی بـه‌عنـوان یـک سـکوی ارتبـاطی (ابزارهای فنی / سیستم‌های اطلاعاتی) صحبت به میان می‌آیـد و یـا اینکـه بـه تعـاملات میـان بازیگران اطلاعاتی که محتوا ایجاد می‌کنند (خود اطلاعات) اشاره دارد، امری دشوار است.

اصلح است که اصطلاح «رسانه‌های اجتماعی» شامل هر دو جنبه، یعنی محتواهایی رسـانه‌هـای اجتماعی که با استفاده از سکوهای اجتماعی فناورانه منتشر یـا بـه اشـتراک گذاشـته مـی‌شـود، باشد. به دلیل توانایی‌های بی‌شمار رسانه‌های اجتماعی در تکرار اطلاعات با سرعت‌های بـالا و هزینه‌های پایین و همچنین چالش‌های تفکیک واقعیت از روایت‌هـای سـاختگی دسـت‌کـاری شده به دلیل مشکلاتی که در ردیابی درستی و منبـع ایـن اطلاعـات وجـود دارد، رسـانه‌هـای اجتماعی می‌توانند برای دستیابی به نتایج نظامی خاص استفاده شوند کـه در بخـش بعـدی در مورد آن بحث خواهد شد.

مبانی نظری

مسلح سازی رسانه‌های اجتماعی

رسانه‌های اجتماعی می‌توانند به شش روش در پشتیبانی از عملیات نظامی بکار گرفته شوند– جمع‌آوری اطلاعات، هدف‌گیری، القاء کردن و تأثیرگذاری (جنگ روانی)، عملیات سایبری، دفاع و فرماندهی و کنترل. همه این فعالیت‌ها، صرف‌نظر از اینکه اثرات آنلاین یا آفلاین دارند، می‌توانند از طریق رسانه‌های شبکه‌های اجتماعی اجرا شوند. این فعالیت‌ها، پشتیبان فعالیت‌های دیگر بوده و اغلب می‌توانند در هماهنگی با فعالیت‌های فیزیکی در زمین انجام شوند.



شکل ۱: مسلح سازی رسانه‌های اجتماعی

در ادامه هر یک از شش روش به‌اختصار معرفی می‌گردند.

۱- هدف‌یابی[1]

هدف‌یابی عبارت است از استفاده از رسانه‌های اجتماعی در شناسایی اهداف بالقوه برای اقدامات نظامی در قلمرو فیزیکی (بر اساس برچسب‌های جغرافیایی تصاویر یا مکالمات جاری در رسانه‌های اجتماعی) و نیز حمله به حساب‌های کاربری رسانه‌های اجتماعی از طریق هک کردن یا پاک کردن یا تغییر شکل آن‌ها. برای مثال استفاده از گوگل‌مپ و تلفن‌های همراه سربازان لیبی توسط ناتو برای موقعیت‌یابی آنان و یا حمله به مراکز فرماندهی داعش توسط نیروی هوایی ایالات‌متحده که از ردیابی پست‌های اعضاء داعش در رسانه‌های اجتماعی تا اجرای عملیات تنها ۲۲ ساعت به طول انجامید.

۲- جمع‌آوری اطلاعات[2]

جمع‌آوری اطلاعات عبارت است از جستجوی متمرکز به‌منظور تجزیه‌وتحلیل اطلاعات به‌دست‌آمده از شبکه‌ها و پروفایل‌های رسانه‌های اجتماعی از جمله محتواها و مکالمات در راستای پشتیبانی از جنگ روانی یا انتخاب اهداف برای عملیات آنلاین یا فیزیکی. این اقدامات

1. Targeting
2. Intelligence Collection

ممکن است پنهانی یا آشکارا صورت گیرند. تجزیه تحلیل بر روی روندها، شبکه، عواطف، جغرافیا، رفتار، سیستم و اطلاعات و آنالیز مخاطب هدف صورت می‌گیرد. از جمله چالش‌های این روش، ملاحظات قانونی و اخلاقی نظیر نقض محرمانگی و وجود نویز در جریان‌های داده‌ای و چالش اندازه‌گیری میزان تأثیر مباحثات آنلاین بر رویدادهای آفلاین می‌باشند. برای مثال بیان اغراق‌آمیز نقش توییتر در بهار عربی.

جمع سپاری[1] به‌منظور بررسی حقیقت و نمایان کردن اطلاعات دروغین نه‌تنها در جمع‌آوری و تحلیل اطلاعات بلکه به‌عنوان ابزاری در جنگ اطلاعات به‌منظور آشکار کردن حقیقت با جمع سپاری اطلاعات به عموم مردم بکار می‌رود. برای مثال: حضور سربازان روسیه در خاک اوکراین از طریق موقعیت‌یابی پروفایل سربازان روس، گوگل‌مپ و برچسب مکانی تصاویر منتشرشده آنان و جمع سپاری اطلاعات شاهدان عینی، آشکار گردید.

۳- دفاع[2]

منظور از دفاع، محافظت از سکوهای رسانه‌های اجتماعی، سایت‌ها، پروفایل‌ها و حساب‌های کاربری در سطح فنی یا سیستمی می‌باشد. اقدامات دفاعی ممکن است شامل استفاده *از رمزنگاری، ضد ردیابی*[3] *و یا نرم‌افزار پنهان* کردن IP در رسانه‌های اجتماعی باشند. برای مثال، نداشتن درک از امنیت عملیات و فقدان آگاهی در مورد امنیت سایبری به قیمت جان بسیاری از یاغیان در سوریه تمام شد. سازمان‌های تروریستی غالباً از سکوهای گپ و گفت رمز شده برای ارتباط و افراطی کردن بیشتر حامیان خود استفاده می‌کنند. ردیابی پلی‌استیشن به‌عنوان یکی از چالش‌برانگیزترین سکوهای بازی برای سرویس‌های اجرای قانون شناخته شده است زیرا اغلب مجرمان از این سکو برای برقراری ارتباطات با یکدیگر استفاده می‌کنند. گواه دیگر بر این موضوع آن است که داعش به اعضاء خود در مورد خطرات بی‌توجهی به امنیت سایبری هشدار داده و در دسامبر ۲۰۱٤ فرمانی مبنی بر ممنوعیت روشن کردن برچسب جغرافیایی[4] توییتر به جنگجویان خود صادر نمود. همچنین داعش یک میز خدمات آنلاین و راهنمای محرمانگی ایجاد نمود که توصیه‌هایی برای نحوه اطمینان یافتن از امنیت عملیات در محیط

1 . Crowdsourcing
2 . Defence
3 . Anti-tracking
4 . geo-tagging

مجازی ارائه می‌داد. به‌عنوان مثالی دیگر اقدامات گروه هکتیویست آنینیموس[1] در جهت هک کردن حساب‌های رسانه‌های اجتماعی داعش در پاسخ به حملات تروریستی آنان در پاریس قابل ذکر است. داعش برای حفاظت از حامیان خود پیامی را در تلگرام توزیع نمود که پنج نکته برای اقدامات احتیاط‌آمیز برای جلوگیری از هک شدن به آن‌ها ارائه می‌داد (شکل ۲).

شکل۲: اقدامات احتیاطی داعش برای اعضاء خود در تلگرام

٤- القاء کردن و تحت تأثیر قرار دادن (جنگ روانی)

جنگ روانی به معنای انتشار اطلاعات به‌منظور تأثیرگذاری بر ارزش‌ها، سیستم اعتقادی، ادراک، احساسات، انگیزه، استدلال و رفتار مخاطب هدف می‌باشد. استفاده از رسانه‌های اجتماعی در جنگ روانی ممکن است در پی دستیابی به اثرات معین نظامی در قلمرو شناختی – شکل دادن، القاء کردن، تأثیرگذاری، دست‌کاری، افشاء، کوچک نمائی، ترویج دادن، فریب دادن، وادار کردن، بازداشتن، بسیج کردن و متقاعد کردن– باشد.

روش‌های جنگ روانی ممکن است آشکار باشند نظیر ایجاد اکانت‌ها، کانال‌ها، وب‌سایت‌ها و اظهارنظرها (کامنت‌ها) توسط رهبران عقاید؛ یا ممکن است پنهانی باشند نظیر هویت‌های جعلی، بات‌نت‌ها[2] و اوباشگری اینترنتی[3]؛ یا ممکن است با هر ترکیبی برای عملیات اطلاعاتی در رسانه‌های اجتماعی بکار رود.

1. Anonymous
2. botnets
3. trolling

برخی از روش‌های جنگ روانی در رسانه‌های اجتماعی عبارت‌اند از:

– **افزایش قابلیت دیده شدن پیام**: استفاده از محتوای به‌طور خودکار تولیدشده از طریق هرزنامه‌ها و استفاده از هویت‌های جعلی برای انتشار یک پیام و کمینه‌کردن اظهارات جایگزین که شامل روش‌های زیر هستند:

- بمب‌های توییتری[1]: ارسال یک‌باره هزاران پیام مشابه در توییتر.
- حساب زاپاسی‌ها[2]: کسانی که یک یا چند حساب غیر از حساب اصلی خود در رسانه‌های اجتماعی دارند.
- اوباشگری اینترنتی[3]: اجیر کردن عده‌ای مزدور یا گروه‌های بی‌طرف به‌منظور پاسخگویی به پست/پست‌هایی که در رسانه‌های اجتماعی توسط یک فرد یا از طرف یک سازمان یا دولت، انتشاریافته است، از طریق ارسال پاسخ‌ها (کامنت‌ها) یی در مخالفت با این پست‌ها.
- بات‌ها[4]: نوعی حساب کاربری ویژه هستند که برای ارسال و دریافت خودکار پیام طراحی می‌شوند.
- اشباع محیط اطلاعاتی: استفاده هماهنگ از بلاگ‌ها، پست‌ها، مقالات و غیره که توسط رهبران عقیده، فعالان یا شخصیت‌های جعلی پست و پست مجدد می‌شوند.
- ربودن هشتک‌های مورد توجه در رسانه‌های اجتماعی: به‌منظور افزایش رساندن پیام به مخاطبان یا گمراه کردن مخاطبان؛ برای مثال داعش از هشتک napaquake (پست‌های مربوط به زلزله اخیر در شمال کالیفرنیا) برای پست کردن تصاویر و پیام‌های تهدیدآمیز خود علیه ایالات‌متحده استفاده می‌کرد یا از هشتک WorldCup2014 برای به اشتراک‌گذاری محتواهای طرفداری از داعش علاوه بر هشتک‌های مختلف مختص داعش استفاده می‌کرد.

– **هدف‌گیری و گیج کردن مخالفان**: توزیع اطلاعات غلط و شایعات، به‌منظور در معرض عموم قرار دادن خطاکاری دشمن. برای مثال در درگیری روسیه و اوکراین، طرفداران

1 . Twitter-bombs
2 . sock puppets
3 . trolling
4 . Bots

روسیه به‌طور نظام‌مند ترس، اضطراب و بیزاری را در میان نژاد روس (و سایر جمعیت‌های غیر اوکراینی) نسبت به اوکراین ایجاد نمودند.

- حمله به هدف، مسدود کردن محتوای دشمن یا درخواست از سکوهای رسانه‌های اجتماعی برای حذف محتوای پروفایل‌هایی خاص از طریق گزارش کردن[1] (دروغین) خطرات امنیتی محتوای آن پروفایل‌ها.

برای مثال تصویر دختربچه اوکراینی (شکل ۳) که در مراسم یادبود پدرش، یک سرباز اوکراینی که در غرب اوکراین کشته شده بود، بعدازآنکه کاربران رسانه‌های اجتماعی طرفدار روسیه، این پست را حاوی محتوای نامناسب (خشونت‌آمیز) گزارش نمودند، توسط مدیران فیس‌بوک حذف گردید.

شکل۳: تصویری که پس از گزارش دروغین کاربران روسی توسط فیس‌بوک حذف گردید

- حملات **شخصی**: به دست آوردن اطلاعات شخصی افراد و استفاده از آن در جهت بدنام کردن، استهزا ء، تهدید یا ترساندن افراد

روزنامه‌نگار فنلاندی که از سیاست‌های روسیه انتقاد کرده بود، تجارب خود را در خصوص حملات ترول به او در رسانه‌های اجتماعی و مورد استهزاء قرار دادن زندگی شخصی و حرفه‌ای خود توسط عوامل روسیه بازگو نمود.

1 - report

- **مهندسی اجتماعی:** در قلمرو سایبر به معنی دست‌کاری روانی افراد برای انجام اعمالی خاص یا افشاء اطلاعات دارای طبقه‌بندی است. مجرمان سایبری اغلب از مهندسی اجتماعی به‌منظور کشف اطلاعات لازم برای دستیابی به یک سیستم، کلاه‌برداری یا سایر حملات استفاده می‌کنند.

این روش‌ها برای اهداف نظامی نظیر جاسوسی و جمع‌آوری اطلاعات نیز بکار می‌روند. ممکن است به‌طور خودکار توسط بات‌ها یا توسط انسان‌ها با هویت‌های جعلی انجام شود.

برای مثال ***catfishing*** (تطمیع با هویت‌های تخیلی برای ایجاد روابط رمانتیک با افراد در اینترنت) سربازان استرالیایی توسط طالبان: طالبان با ایجاد اکانت‌های جعلی به نام زنان جذاب و برقراری ارتباط با سربازان استرالیایی توسط آنان به استخراج اطلاعات از این سربازان اقدام می‌کرد که این عملیات بعداً ممکن بود در عملیات مورد استفاده قرار گیرند.

- **فریب:** ایجاد نویز یا مِه اطلاعاتی[1] حول یک موضوع برای منحرف کردن توجه از رویدادهای راهبردی مهم‌تر.

پس از سرنگونی پرواز شماره ۱۷ هواپیمایی مالزی که در میانه راه در مرز روسیه و اوکراین سرنگون شد، کانال‌های رسانه‌ای روسیه و رسانه‌های اجتماعی، حجم بالایی از پیام‌ها را که توضیحات متعددی برای علت این حادثه ارائه می‌داد منتشر نمودند. لیکن یک بات دیگر برای پرت کردن حواس عامه مردم از این ماجرا با توضیحات جایگزین در مورد قتل سیاستمدار روس «بوریس نمسوف» با بیان احتمال کشته شدن او توسط اوکراینی‌های حسود بکار گرفته شد. این اخبار تنها چند ساعت بعد از این حمله انتشار یافت.

۵- فرماندهی و کنترل[2]:

فرماندهی و کنترل عبارت از استفاده از رسانه‌های اجتماعی برای ارتباطات داخلی، به اشتراک‌گذاری اطلاعات، هماهنگی و همگام‌سازی اقدامات می‌باشد. اقدامات فرماندهی و کنترل به‌طور خاص برای عاملان غیردولتی نظیر گروه‌های شورشی به‌ویژه اگر از ساختار رسمی برخوردار نبوده یا از نظر جغرافیایی پراکنده باشند، حائز اهمیت است. از طرفی به دلیل

---

1. Information fog
2. Command and Control(C2)

باز بودن رسانه‌های اجتماعی، غیرمتمرکز بودن گره‌ها یا اهداف فیزیکی، حمله به آنان دشوار است؛ زیرا سکوها و زیرساخت‌ها، نظامی نیستند.

از مهم‌ترین روش‌های فرماندهی و کنترل، تاکتیک‌های ازدحامی[1] هستند که عبارت‌اند از توزیع اطلاعاتی به‌منظور بسیج کردن و هماهنگ کردن عاملان غیردولتی با منافع یا علایق مشترک در جهت درگیری با یک هدف خاص؛ خصوصاً بسیج کردن مردم برای اعتراضات یا تظاهرات قبل از آنکه نهادهای امنیتی فرصت واکنش پیدا کنند. برای مثال، انقلاب‌های بهار عربی و یا اغتشاشات ایران در سال ۸۸ توسط این تاکتیک‌های رسانه‌های اجتماعی نظیر فیس‌بوک و توییتر سازماندهی گردید. گروهک تروریستی داعش نیز بسیاری از اقدامات فرماندهی و کنترل خود را در اپلیکیشن‌های گپ و گفت بسته (نظیر تلگرام) و شبکه‌های بازی هدایت می‌کرد. لیکن برخی از اقدامات خود را در توییتر با هشتک‌های نامرتبطی چون «کشور توییتر (*the state of Twiter*)» منتشر می‌کرد.

٦- عملیات سایبری[2]

عملیات سایبری در رسانه‌های اجتماعی عبارت است از هدف‌گیری سکوها و اکانت‌های رسانه‌های اجتماعی به‌منظور نفوذ به مکان‌های حفاظت‌شده با رمز عبور، تغییر محتوای یک پروفایل یا کاملاً غیرقابل استفاده کردن یک وب‌سایت.

عملیات سایبری ممکن است آفندی یا پدافندی باشند. اگرچه اغلب آن‌ها ذاتاً آفندی هستند. حملات از کار انداختن سرویس توزیع‌شده[3] به وب‌سایت‌ها، هک کردن رمز عبور برای دستیابی به محتوای اتاق‌های گفتگو، ایمیل‌ها یا تلفن‌های همراه یا افشاء محتوای آن‌ها، تغییر محتوای اکانت‌های رسانه‌های اجتماعی، نفوذ به پایگاه داده‌ها برای جمع‌آوری اطلاعات از جمله عملیات سایبری رسانه‌های اجتماعی محسوب می‌گردند. هدف همه این اقدامات جلوگیری از استفاده عاملان مخالف از سکوهای رسانه‌های اجتماعی برای برقراری ارتباط، هماهنگ کردن اقدامات، دستیابی به اطلاعات یا توزیع پیام‌های خود حداقل به‌صورت موقت است.

---

1. Swarming tactics
2. Cyber Operations
3. DDoS

برای مثال، همان‌طوری که در شکل ٤ نشان داده می‌شود، حمله cyberCaliphate به‌حساب توییتر فرماندهی مرکزی ایالات‌متحده[1] و ارسال پیام‌های رعب‌آور به سربازان ایالات‌متحده و حمله به وب‌سایت آژانس خبری آسوشیتدپرس و انتشار اخبار کذب در مورد بمب‌گذاری در کاخ سفید و مصدوم شدن رییس‌جمهور اوباما از جمله عملیات سایبری به رسانه‌های اجتماعی (مطابق شکل ٥) محسوب می‌گردند.

شکل٤: حمله cyberCaliphate به‌حساب توییتر فرماندهی مرکزی ایالات‌متحده

شکل٥: حمله به وب‌سایت آژانس خبری آسوشیتدپرس و انتشار اخبار کذب

– نحوه مواجهه سازمان‌های نظامی با جنگ رسانه‌های اجتماعی

صحنه‌های جنگ نامتعارف، محیط‌های پیچیده‌ای هستند که در آن سازمان‌های نظامی با هزاران هم‌پیمان و دشمن بالقوه مواجه هستند و اغلب تشخیص دوست و دشمن دشوار است. با اضافه شدن عناصر جنگ رسانه‌های اجتماعی، محیط درگیری حتی پیچیده‌تر نیز شده و حفظ

[1] . CENTCOM

امنیت عملیات دشوارتر می‌گردد. سازمان‌های نظامی در جنگ نامتعارف باید با رسانه‌های اجتماعی به روش‌های متعددی سروکار داشته باشند.

- نخست، نیروهای نظامی می‌بایست برای دفاع در برابر حملات نیروهای متخاصم، با به‌کارگیری تدابیر جنگ رسانه‌های اجتماعی علیه آنان، نهادهای هم‌پیمان یا جمعیت‌های داخلی، آماده باشند.
- دوم، نیروهای نظامی می‌بایست برای جنگیدن با نیروهای متخاصمی که از تدابیر جنگ رسانه‌های اجتماعی استفاده می‌کنند، آماده باشند تا تلاش‌های سازمان‌دهی خود را توسعه داده و نیروهای خود را برای مقابله با نیروهای دشمن، تحت تأثیر قرار دهند.
- سوم، کارکنان نظامی می‌بایست در استفاده از تدابیر جنگ رسانه‌های اجتماعی علیه دشمنان خود شامل احزاب شورشی و جمعیت داخلی که از متجاوزان حمایت می‌کنند، از مهارت کافی برخوردار باشند.
- چهارم، سازمان‌های نظامی نیاز به کنترل استفاده اعضاء یا شهروندان کشور خود از رسانه‌های اجتماعی دارند چراکه ممکن است به‌طور تصادفی یا سهواً امنیت عملیات و پایداری کلی نیروهای در حال جنگ را به خطر بیندازند.
- نهایتاً، یک نیروی نظامی باید به‌طور هم‌زمان و در جبهه‌های متعدد قادر به به‌کارگیری تدابیر آفندی و پدافندی جنگ رسانه‌های اجتماعی باشد تا در موقعیت‌های درگیری و صحنه‌های جنگ، پیروز میدان باشد.

نتیجه‌گیری و پیشنهاد

در این مقاله به نحوه استفاده از رسانه‌های اجتماعی در جنگ ترکیبی و نحوه مسلح سازی شبکه‌های اجتماعی پرداخته شد و شیوه‌های مختلف به‌کارگیری رسانه‌های اجتماعی در عملیات نظامی از جمله جمع‌آوری اطلاعات، هدف‌یابی، القاء کردن و جنگ روانی، عملیات سایبری، دفاع و فرماندهی و کنترل به‌طور اجمالی با ذکر نمونه‌های عملی معرفی گردید.

با توجه به افزایش وابستگی به فناوری‌های اطلاعات برای ارتباطات و امور روزمره، استفاده متنوع از فضای سایبری برای مقاصد خیر و شر رو به افزایش خواهد بود. رشد سریع استفاده از اینترنت در سراسر جهان، از جمله استفاده از سکوهای رسانه‌های اجتماعی و اپلیکیشن‌های

تلفن همراه، پیش‌تر این روند را به اثبات رسانده‌اند. در نتیجه، سازمان‌های نظامی با چالش‌های چشمگیری در جنگ رسانه‌های اجتماعی روبرو هستند. یا شاید باید بگوییم، سازمان‌های نظامی یک‌بار دیگر با تأثیر فناوری جدید و در حال تکامل دیگری روبرو می‌شوند. درگیری‌های اخیر نشان می‌دهند که عاملان مختلف چگونه راهبردهای خود را بر اساس تغییر در عادات ارتباطی و توسعه محیط اطلاعاتی انطباق داده‌اند. شگفت‌آور نیست که روش‌های پیچیده‌تر و غیرقابل‌پیش‌بینی‌تری برای تأثیرگذاری بر مخاطبان هدف در آینده استفاده خواهند شد. ویژگی مشترک این درگیری‌ها این است که همگی به‌طور ماهرانه‌ای با محیط اطلاعاتی تطابق یافته و به‌طور مؤثر اقدامات خود را به‌صورت توأمان در فضای فیزیکی و مجازی برای تأثیرگذاری بر نگرش‌ها و رفتارهای مخاطبان هدف ترکیب می‌کنند. به‌علاوه از ابزار و روش‌هایی استفاده می‌کنند که توسط کسب‌وکارهای خصوصی برای مقاصد بازاریابی توسعه یافته‌اند و پیش‌ازاین اثربخش بودن آن‌ها به اثبات رسیده است. عاملان شر، به‌طور مداوم روش‌های جدید و پیچیده‌ای را برای تأثیرگذاری و دست‌کاری افکار عمومی توسعه می‌دهند درحالی‌که سکوهای رسانه‌های اجتماعی نقش اصلی را در این میان به عهده‌دارند. آنچه مسلم است، افزایش حضور در رسانه‌های اجتماعی سودمندتر از تلاش در جهت تضعیف سایر عاملان اطلاعاتی و ایجاد محدودیت در توزیع پیام‌های آنان می‌باشد؛ بنابراین، بی‌توجهی و عدم مشارکت در رسانه‌های اجتماعی دیگر جایز نیست.

نظر به اینکه استفاده از رسانه‌های اجتماعی در جنگ و محیط‌های بدون درگیری به‌سرعت در حال افزایش است، سازمان‌های نظامی در سراسر جهان، بالأخص در ایالات‌متحده، درحال‌توسعه سیاست‌ها و تدابیر رسانه‌های اجتماعی هستند. سازمان‌های نظامی به‌طور خاص نسبت به تدابیر جنگ رسانه‌های اجتماعی آسیب‌پذیر هستند و امنیت عملیات ممکن است به روش‌های بسیاری به خطر بیفتد. در نتیجه اقدامات زیر در جهت بالا بردن توان دفاعی کشور در برابر حملات رسانه‌های اجتماعی به شرح زیر پیشنهاد می‌گردد:

- ایجاد و پشتیبانی از تلاش‌های تحقیقاتی که تهدیدات مترتب بر عملیات نظامی در جنگ رسانه‌های اجتماعی را پوشش می‌دهند.
- گنجاندن مباحث جنگ رسانه‌های اجتماعی در همه برنامه‌های آموزشی و تحصیلی نظامی مرتبط

- افزایش استفاده، مدیریت و پایش محتوای برنامه کاربردی رسانه‌های اجتماعی نظامیان. این کار باید جزء اقدامات مداوم باشد و رویه‌های تجارب و درس آموخته‌ها هم در مورد موفقیت‌ها و هم قصورها باید مورداستفاده قرار گیرند.
- ایجاد یک برنامه انتقال دانش از سازمان‌ها و کشورهای موفق در زمینه جنگ رسانه‌های اجتماعی و بهره‌گیری از کمک و آموزش آن‌ها در زمینه مدیریت و به‌کارگیری رسانه‌های اجتماعی.

فهرست منابع:

- Public report "social medias a tool of hybrid warfare", NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE (2016)
- Thomas Elkjer Nissen (2015), "The Weaponization Of SocialMedia", Royal Danish Defence College
- Public report "New Trends in social Media", NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE (2016)
- Pissanidis. N, Rõigas. H, Veenendaal. M (2016), "The Social Side of 'Cyber Power'? Social Media and Cyber Operations", 2016 8th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn
- TENENBOIM ORI (2017), "Reporting War in 140 Characters: How Journalists Used Twitter during the 2014 Gaza–Israel Conflict", International Journal of Communication 11(2017), 3497–3518
- Erbschloe, Michael (2017), "Social media warfare _ equal weapons for all", CRC_Taylor & Francis_ Auerbach Publications