

تأثیرات مثبت و منفی شبکه‌های اجتماعی بر امنیت ملی کشورها با تکیه بر مهندسی اجتماعی

حسن ویشته

دانشجوی دکتری مدیریت راهبردی پدافند غیرعامل دانشگاه عالی دفاع ملی

تهران، ایران

vishte@sndu.ac.ir

چکیده

امروزه گسترش فناوری اطلاعات و ارتباطات و کاربردهای آن به گونه‌ای توسعه یافته که حداقل در جوامع پیشرفته در تمامی شئون زندگی افراد و اکثر فعالیت‌های اجتماعی، فرهنگی، اقتصادی و حتی سیاسی وارد شده است. و به تدریج فضای سایبر را به عنوان یک ابزار تسهیل کننده برقراری امنیت یا ایجاد یک فضای ناامن معرفی کرده است. بر اثر گسترش استفاده از اینترنت و حاکم شدن فضای سایبری در مناسبات اجتماعی و سیاسی هم اکنون شبکه‌های اجتماعی* چالش اصلی حکومت‌ها در امنیت جامعه اطلاعاتی می‌باشند چرا که مردم مهمترین تولید کنندگان، مصرف کنندگان و توزیع کنندگان اطلاعات در محیط شبکه‌های اجتماعی مجازی هستند. شعار یا لوگوی پنهان همه شبکه‌های اجتماعی یک جمله است: "اگر می‌خواهید همه جا باشید، بگذارید همه به اطلاعات شما دسترسی داشته باشند" به عبارتی یا شما همه جا باشید یا اجازه بدهید همگان (از همه جا) اینجا باشند و این یعنی ماده خام برای اجرای تئوری جاسوسی عمومی. زیرا کاربر در شبکه‌های اجتماعی به بهانه داشتن ارتباطات گسترده، مدام در حال ارائه اطلاعات شخصی خود (و جامعه خود) به شکل عمومی است! در سال ۲۰۰۶ بین ۴ تا ۵ میلیون ایرانی در جهان پراکنده بودند. که بنا به گزارش بنیاد سیاست مهاجرت (migration policy institute) در بین کشورهایی که بیشترین مهاجرین ایرانی را در خود جای داده اند آمریکا رتبه اول و پس از آن کانادا، آلمان، سوئد و اسرائیل قرار دارند. این مهاجرین علاقه وافری به عضویت در شبکه‌های اجتماعی داشته به گونه‌ای که در سال ۲۰۰۵ ایرانی‌ها سومین رتبه را در شبکه اورکات[†] داشتند و از طرفی به دلیل فرهنگ خاص ایرانیان صفت زودجوش بودن و اعتماد به دیگران بخصوص اعضای فامیل نوعی ارزش کاذب محسوب می‌گردد که این حالت سبب تبدیل فرد به یک طعمه در روش‌های مهندسی اجتماعی است. در واقع مهندسی اجتماعی سوءاستفاده زیرکانه از تمایل طبیعی انسان به اعتماد کردن است، که به کمک مجموعه‌ای از تکنیک‌ها، فرد را به فاش کردن اطلاعات یا انجام کارهایی خاص متقاعد می‌کند. [1] تکنیک‌های مهندسی اجتماعی یکی از ابتدایی ترین اما در عین حال زیرکانه ترین روش‌های نفوذ و دستیابی به اطلاعات می‌باشد. که از طریق شبکه‌های اجتماعی ضریب نفوذ این تکنیک‌ها از سطح محلی و کشوری ارتقاء یافته و بین‌المللی شده است.

واژگان کلیدی

امنیت، شبکه‌های اجتماعی، مهندسی اجتماعی.



۱- مقدمه

" کنترل و نظارت بر شبکه‌های اجتماعی جز لاینفک امنیت ملی و از ضروریات برقراری و حفظ امنیت در سطح بین المللی است". [4]

۲- ادبیات موضوع:

- **ویژگی‌های شبکه‌های اجتماعی:** مجموعه‌ای از ویژگی‌های این شبکه‌ها باعث شده است که نسبت به ارتباط واقعی اجتماعی تاثیر گذار بیشتری داشته باشند که مهمترین آنها عبارتند از: تولید هویت مشترک و بعضا جدید و مثبت^۵، به اشتراک گذاری و یادگیری، تسهیل انتقال فرهنگ و باورها، قدرت ایجاد تحرک و یا جنبش اجتماعی، چند رسانه‌ای بودن، جهانی بودن، سرگرمی، جستجو کردن و جستجو شدن، ابتکار و خلاقیت^۶

- **اهداف شبکه‌های اجتماعی:** اهداف ظاهری این شبکه‌ها بیشتر بر اساس همان ویژگی‌هایشان برقراری ارتباط با دوستان سابق و ایجاد ارتباط دوستانه پنهان و آشکار در سطح گسترده، بیان عقاید در فضای آزاد و بدون چون و چرا و استفاده رایگان از امکانات آموزشی، تفریحی این شبکه‌ها است. و متخصصین روانشناسی مشاور طراحان این شبکه‌ها^۷ با کمک به ایجاد یک تصویر مثبت و تاثیر گذار از کاربران به نوعی اعتماد به نفس کاذب در کاربران ایجاد می‌کنند که جاذبه شدیدی برای نسل جوان ایجاد کرده است.

شبکه اجتماعی ساختاری است از افراد و سازمانها که بواسطه علایق، سلايق، عقاید و منافع مشترک با یکدیگر ارتباط دارند. مردم می‌توانند در آن اندیشه‌ها، خواسته‌ها، دل‌بستگیها و کارهایشان را به اشتراک بگذارند. شبکه‌های اجتماعی زیر مجموعه **رسانه اجتماعی**^۱ محسوب می‌شوند. این شبکه‌ها با در اختیار گذاردن مجانی امکاناتی خاص نظیر پست الکترونیکی (خبر نامه‌های الکترونیکی)، کتابخانه‌های مجازی، بخشهای آموزشی، ارائه خدمات جهت شرکت در کنفرانسها و مجامع بین المللی و..... جوانان زیادی را به سمت خود جذب نموده اند. اهداف ظاهری این شبکه‌ها بیشتر بر اساس همان ویژگی‌هایشان برقراری ارتباط با دوستان سابق و ایجاد ارتباط دوستانه پنهان و آشکار در سطح گسترده، بیان عقاید در فضای آزاد و بدون چون و چرا و استفاده رایگان از امکانات آموزشی، تفریحی این شبکه‌ها است. لذا در جوامع مسلمان که بدلیل اعتقادات مذهبی یا محدودیتهایی اجتماعی ارتباط نوجوانان و جوانان از جنس مخالف مقدور نیست با سرعت شدیدی نسبت به سایر جوامع گسترش یافته است. گردانندگان این شبکه‌ها در واقع در صدد شکل دادن و هدایت افکار جوانان و در نهایت کنترل جوامع هستند. و گرچه در ابتدا این هدف را پنهان می‌نمودند ولی هم اکنون به صورت واضح این موضوع را اعلام می‌کنند شعار فعلی گردانندگان فیس بوک چنین است:

" we are the social net work generation and we will control the world
" ما نسل شبکه‌های اجتماعی هستیم و ما جهان را کنترل می‌کنیم"
[2].

بعنوان مثال موسسه بین المللی مشاوره‌های رسانه‌ای CIMA^۲ تحقیقات جامعی در خصوص نقش شبکه‌های اجتماعی در جنبشهای اجتماعی جهان عرب انجام داده و در آنها نقش انکار ناپذیر این شبکه‌ها در برقراری ارتباط بین انقلابیون، انتقال اخبار به خارج از کشور و همچنین بسیج شهروندان^۳ مورد تاکید قرار گرفته است. [3]
به همین دلیل است که در یکی از تحقیقاتی که دانشگاه دفاع ملی آمریکا^۴ اخیراً نتایجش را منتشر کرده است اعلام می‌گردد:

⁵-positive self image

⁶-university of pacific , www.pacific.edu

⁷-network generators

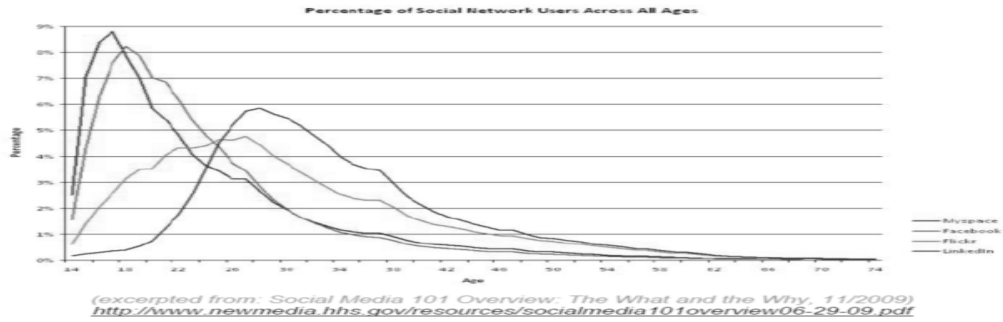
¹-Social media

²-center for international media assistance

³-citizen mobilization

⁴-The national defense university





شکل شماره ۱: مقایسه پراکندگی سنی چهار شبکه اجتماعی MySpace-Flickr-Facebook-LinkedIn [6]



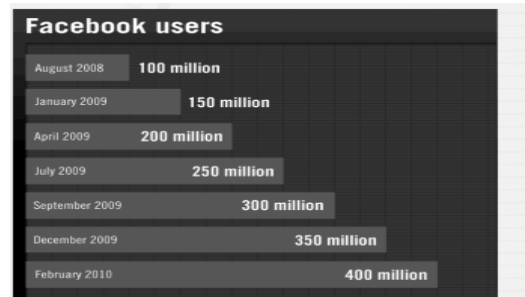
شکل ۳: نقشه پراکندگی جغرافیایی کاربران شبکه‌های اجتماعی مختلف در سال ۲۰۱۱ [10]

رشد فزاینده فیس بوک در سطح بین المللی بسیار عجیب به نظر می‌رسد " روبین واوتر" از متخصصان برجسته شبکه‌های اجتماعی در مقاله‌ای تحت عنوان " برتری بلامنازع و ابدی فیس بوک " می‌نویسد:

این شبکه در فوریه ۲۰۰۴ در سطح دانشجویان هاروارد تاسیس شد و سایر شبکه‌ها با احساس خطر از جانب آن سعی در متوقف کردن این شبکه نمودند. در عرض کمتر از یکسال Friendster تلاش کرد این شبکه را به قیمت ۱۰ میلیون دلار خریداری کند که موفق نشد و در سال ۲۰۰۶ یاهو قیمت خرید را یک میلیارد دلار افزایش داد و هم اکنون ارزش تقریبی این شبکه تا حدود ۲.۳ میلیارد دلار تخمین زده می‌شود. این متخصص پیش‌بینی می‌کند تا پایان ۲۰۱۲ تعداد کشورهایی که این شبکه برتری کامل خواهد یافت به رقم خیره کننده ۱۱۵ کشور از ۱۳۲ کشور خواهد رسید. [11]

در ج.ا.ایران دومین تهدید در مجموع تهدیدات شبکه‌های اجتماعی وبلاگها هستند. وبلاگها در ۱۹۹۹ شروع بکار کردند و در ایران در شهریور ۱۳۸۰ اولین وبلاگ فارسی توسط " سلمان جریری " بر

شکل شماره ۱: نشاندهنده اقبال اجتماعی گروههای سنی مختلف به این شبکه‌ها است. رشد فزاینده این شبکه‌ها یک پدیده جهانی است. آمار رسمی نشان می‌دهد که استفاده کنندگان از فیس بوک از اگوست ۲۰۰۸ تا فوریه ۲۰۱۰ چهار برابر شده است. [7]



شکل ۲: افزایش تصاعدی کاربران face book در کمتر از دو سال

آمار منتشره در سایت دیده بان شبکه‌های اجتماعی^۱ اعلام میکند که ۸۲٪ از افراد استفاده کننده از اینترنت که بالای ۱۵ سال سن دارند با شبکه‌های اجتماعی ارتباط دارند. [8] در حال حاضر بزرگترین شبکه اجتماعی از نظر تعداد کاربران "شبکه فیس بوک" است که در منطقه خاورمیانه و کشور جمهوری اسلامی ایران هم این شبکه غالب است. البته نقشه پراکندگی کاربران این شبکه‌ها در چند سال گذشته به شدت متغیر بوده است. [9]

^۱.social networking watch

ساده یا یک عکس قابل استخراج است برای کاربر معمولی قابل تصور نیست. چنانکه در تصویر روبرو ملاحظه می‌شود با یک ارتباط ساده در یک شبکه اجتماعی و بارگذاری^۵ تنها یک عکس این اطلاعات قابل استخراج است: نام و محل زندگی شخص، محل خدمت، عضویت در نیروی هوایی، اسامی دوستان، که احتمالا^۶ روسا و مسئولین واحد نظامی مربوطه را هم شامل می‌شود. این اطلاعات وقتی که با اطلاعات استخراج شده از دوستان این شخص تجمیع شود نتایج خیره کننده خواهد بود به همین علت به مواردی برخورد می‌کنیم که ارتش امریکا یا اسرائیل به دلیل انتشار یک عکس حکم بازداشت نیروی مربوطه را صادر نموده است.

What can we find here?

How often the page is monitored
Air Force Members?
Where they served
All their friends

Reverse Engineer Static Reversing and Vulnerability Analysis. Your dream job? osintia.com
Social Media Experts Need help building your online community? Buzz on us on 01582 480126 www.osintia.com
AGT International A Global Provider of Advanced Safety and Security Solutions www.agtinternational.com
smart by TAB Systems Inc biometric access control, time & attendance and building automation www.tab-systems.com

شکل ۴: اطلاعات استخراج شده از نمایش تنها یک عکس در شبکه‌های اجتماعی

Israeli jailed for Facebook photo

Israel has sentenced a soldier to 19 days in jail for uploading a photograph taken on his military base to the social networking website, Facebook.

The Israeli military declined to comment on the nature of the image.



شکل ۵: خبر بازداشت سرباز اسرائیلی به علت انتشار یک عکس در فیس بوک.

[13]

روی صفحه اینترنت گذاشته شد. در یکسال اول تنها ۱۵۰۰۰ نفر اقدام به راه اندازی وبلاگ کردند ولی هم اکنون پس از زبانهای انگلیسی، پرتغالی، لهستانی زبان فارسی در رتبه چهارم زبانها در وبلاگ نویسی است. دلایل فراوانی برای این اقبال زیاد در ایران وجود داشته باشد ولی مهمترین آنها عبارتند از اینکه در وبلاگ نویسی اطلاعات کامپیوتری اندکی نیاز است و راه اندازی آن در اکثر کشورها تقریباً^۷ هزینه‌ای ندارد. از طرفی چون هویت وبلاگرها کاملاً شناخته نمی‌شود لذا نویسندگان بسیار بی پروا و جسورانه مطالب و اندیشه‌های خود را بیان می‌کنند. همچنین چون قابلیت به روز شدن وبلاگها بسیار بالاست در بسیاری از کشورها جدیدترین اطلاعات از طریق این وبلاگها در دسترس قرار می‌گیرد به گونه‌ای که وقتی در ۱۴ دسامبر ۲۰۰۳ ساعت ۵ صبح خبر دستگیری صدام حسین منتشر شد در عرض مدت کوتاهی عکس و تفصیلات خبر در وبلاگها منتشر شد در حالیکه قویترین روزنامه‌های آمریکایی پس از گذشت ۱۰ ساعت توانستند ویژه نامه خبری خود را ارائه دهند. [۱] به گزارش خبرگزاری موج ج.ا. ایران با آمار ۷۰۰ هزار وبلاگ موجود (۴۰۰ هزار فعال) در رتبه نهم دنیا قرار دارد که در مقایسه با آلمان با ۳۰۰ هزار و هندوستان با یکصد هزار وبلاگ رقم بزرگی است و باعث شده است تا "پرشین بلاگ" با تعداد کاربر ۵۲۰ هزار در سطح بین المللی در رتبه سیزدهم جای گیرد. [12]

سه دسته تهدید اصلی که در بستر شبکه‌های اجتماعی بوقوع می‌پیوندد عبارتند از:

۱- اطلاعات در دسترس! وقتیکه شما در یک شبکه اجتماعی علی‌الظاهر با یک دوست در ارتباط هستید تصور می‌کنید اطلاعات شما در اختیار یک نفر قرار می‌گیرد ولی در واقع تعداد نامحدودی^۲ از افراد به اطلاعات شما دسترسی داشته و سیستم با تطبیق^۳ اطلاعات شما با اطلاعات قبلی و اطلاعات دوستان شما در واقع به اطلاعات کامل و اصیل دسترسی پیدا می‌کند. جریان شبکه‌های اجتماعی یک جریان تجاری است که با بهره برداری تجاری از اطلاعات کاربران به حیات خود ادامه می‌دهد. و از طرفی تشخیص واقعی و یا دروغ^۴ بودن اطلاعات برای کاربران غیر ممکن است و معمولاً آنچه که از یک پیام

^۱- open intel information

^۲- x number

^۳-match up

^۴-fake or real

^۵-upload

خاستگاه ومنشاء اولیه این شبکه‌ها بوده است و وزارت امنیت داخلی^۶ (DHS) رسماً این شبکه‌ها را رصد می‌کند. شبکه خبری CBS در مقاله‌ای تحت عنوان "وزارت امنیت داخلی اطلاعات شبکه‌های اجتماعی را درو می‌کند" اعلام کرده است که بنا بر تحقیقات کلینیک ساموئلسون در دانشگاه برکلی^۷ حداقل شش آژانس امنیتی تحت نظر دولت شبکه‌های اجتماعی را رصد میکنند و مجموعه اطلاعات، تحلیلها و بررسی آنها در "مرکز پایش شبکه‌های اجتماعی^۸ نگهداری می‌گردد. [14]

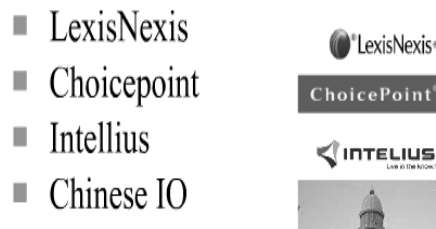
خبرگزاری رویترز در مقاله‌ای به قلم نویسنده معروف Eric Walsh اعلام می‌کند: بنا بر اسناد رسمی از DHS این وزارتخانه به صورت منظم کلیه اطلاعات شبکه‌های اجتماعی، سایتهای خبری^۹ اطاقهای اطاقهای گفتگو و سایتهای تفریحی شایعه^{۱۰} را حداقل از ژوئن ۲۰۱۰ بررسی و پایش کرده است. و به کاربران شبکه‌های اجتماعی نوید داده می‌شود که اطلاعات بررسی شده به صورت دائم و همیشگی نگهداری نمی‌شوند بلکه حداکثر تا مدت ۵ سال ذخیره می‌گردند. البته در این پایش بعضی از موضوعات بطور ویژه مورد بررسی قرار می‌گیرند مثلاً "کلیه وبلاگهایی که راجع به مهاجر^{۱۱} - مشکلات مرزی- بیماری آنفلونزای پرندگان^{۱۲} و... مطلب می‌نویسند. و از نکات جالب توجه اینکه در ذیل عنوان بررسی وبلاگ jihad watch اذعان می‌کند که کلیه اطلاعات مرتبط با جهان اسلام که در شبکه‌های اجتماعی منتقل می‌شوند بطور جداگانه بررسی می‌گردند. [15]

سایت رسمی یکی از زیر مجموعه‌های وزارتخانه امنیت داخلی در ژانویه ۲۰۱۲ در مطلبی تحت عنوان: "سیاست پایش شبکه‌های اجتماعی زیر آتش انتقاد"^{۱۳} می‌نویسد:

این یک تاکتیک کسب اطلاعات امنیتی از طریق شبکه‌های اجتماعی^{۱۴} است و DHS مجاز است که علاوه بر پایش کلی اطلاعات جابجا شده در این شبکه‌ها به صورت انفرادی از نام کاربری هر کاربر استفاده کرده و موضوعات یا عناوینی نظیر تروریسم، موادمخدر و آدم ربایی و... را جستجو کند ولی مجاز به ارسال اطلاعات،

۲- **تعیین مکان جغرافیایی کاربر^۱**: موضوع دیگر که در بحث شبکه‌های اجتماعی حائز اهمیت است موضوع مشخص کردن مکان دقیق کاربر است. با توجه به اینکه مکانیابی دقیق کاربر یکی از اهداف تجاری شبکه‌ها به منظور نیل به هدف بازاریابی برتر^۲ است. لذا تمام شبکه‌ها این اطلاعات را با روشهای مختلف، از قبیل سئوالات فراوان و هدفدار- تنظیمات زبان و مکان کامپیوتر- آدرس اشتراک دهنده اینترنت و... از کاربر اخذ می‌کنند.

۳- **"تجمیع کنندگان اطلاعات"**: داده‌های جمع آوری شده از کاربران به صورت کلی و بدون ذکر نام تک تک افراد به شرکتی که تحت عنوان "تجمیع کنندگان اطلاعات شناخته می‌شوند فروخته می‌شوند. که آنها پس از تطبیق و ارتقا این داده‌ها اطلاعات بدست آمده را به "شرکتهای اشتراک پذیر"^۳ می‌فروشند بسیاری از ما علامت تجاری این شرکتها را در بالای صفحاتی که در اینترنت مشاهده می‌کنیم دیده ایم و شاید برای ما سؤال پیش آمده که آنها چه معنایی دارند. در حال حاضر چهار اشتراک پذیر بزرگ و اصلی در این رابطه عبارتند از:



شکل ۵: نام و نشان تجاری چهار شرکت بزرگ اشتراک پذیر

ودرنهایت این اطلاعات به شرکتیهای فعال در صنعت تبلیغات اینترنتی^۴ فروخته می‌شود. که این صنعت خود شامل چند گروه شرکتیهای مختلف با تخصصهای مختلف است. بدیهی است وقتیکه چنین مجموعه‌ای از اطلاعات پردازش شده راجع به مردم یک شهر- کشور - منطقه یا قاره مورد خرید و فروش قرار می‌گیرد این شکار بزرگ از دسترس سازمانهای جاسوسی - امنیتی و حتی از دسترس هکرای حرفه‌ای در امان نخواهد بود. در ایالات متحده آمریکا که

6 -Department of homeland security

7 -Berkeley's Samuelson clinic

8 -social networking monitoring center

9 news sites-

10 Gossip sites-

11 Migration-

12 Bird flu-

13 Social media monitoring policy under fire-

14 Tactics of gathering intelligence via social media-

1- Geo location

2 -hyper marketing

3- information aggregators-

4--subscriber

5- online advertiser companies

ضمن تاکید بر خطر به سرقت رفتن اطلاعات با روشهای مهندسی اجتماعی، از پرسنل دولتی خواسته شده است هر چه کمتر اطلاعات شخصی خود منجمله آدرس منزل-شماره تلفن، اطلاعات حسابهای بانکی و شماره امنیتی اجتماعی⁸ و عکسهای گرفته شده در محیطهای کاری را در این سایتها قرار دهند. [19] و متعاقباً وزارت امنیت داخلی (DHS) اقدام به انتشار "سیاستهای اجرایی پرسنل دولتی برای شبکههای اجتماعی"⁹ نموده است. که نشان می دهد گر چه این وزارتخانه با تصویب سریع قوانین جدید کاملاً جریان اطلاعات منتقله در این شبکهها را پایش می کند ولی ایالات متحده آمریکا از همین منظر به شدت احساس آسیب پذیری می کند. در واقع به نظر می رسد شبکههای اجتماعی تبدیل به یک سلاح مرگبار در جنگ نرم و فعالیتهای جاسوسی شده که قابلیت استفاده علیه سازندگان اصلی را هم دارد. و ما می توانیم از این قابلیت به نحو احسن در جهت اشاعه افکار حق طلبانه خود و دفاع از حقانیت انقلاب اسلامی بهره برداری کنیم. یک متخصص برجسته آمریکایی در امور امنیت و تکنولوژیهای جدید¹⁰ به نام لوییس شفرد می نویسد:

در انتخابات اخیر ایران، مسئولین ایرانی ابتدا سعی کردند با روش فیلتر کردن با قدرت فزاینده شبکه فیس بوک مقابله کنند که از نظر ما یک شکست برای آنها بود ولی ایرانیها به سرعت استراتژی خود را عوض کردند و تلاش کردند از بستر شبکه فیس بوک تبلیغات ضد غربی¹¹ (anti-western propaganda) خود را اشاعه دهند و این یک خطر است [20].

متخصص آلمانی الاصل به نام میسایل ورتهایمر¹² که در حال حاضر در اداره کل آنالیز امنیت ملی آمریکا¹³ فعالیت می کند معتقد است که بهترین راه برای بدست آوردن اطلاعات دقیق در موضوعاتی که در سایر کشورها اتفاق می افتند، استفاده از شبکههای اجتماعی است. برای اینکار می توان یک فضای مجازی در شبکه برای یک موضوع ایجاد کرد و بعد به تجزیه و تحلیل اطلاعات جمع شده از نظرات کاربران پرداخت. و از جمله مواردی که از این تکنیک

پذیرش دعوتنامه های دوستان و یا تماس با ایشان نیست. همچنین این وزارتخانه مجاز است که در رابطه با افراد نسبت به جمع آوری ذخیره کردن، تجزیه و تحلیل و در صورت لزوم انتشار یا ارائه این اطلاعات به مسئولین حکومتی آمریکا در سطح ملی، ایالتی، منطقه ای، و حتی دولتهای خارجی و بخش خصوصی اقدام نماید. [16]

یکی از مسئولین سابق FBI که با این مرکز همکاری می کند ضمن اظهار تعجب از حجم اطلاعات قابل دسترس در مورد زندگی خصوصی افراد در این شبکهها، بهره برداری سازمانهای امنیتی از این اطلاعات را کاملاً طبیعی و استاندارد اعلام کرده و از آنها بعنوان منابع عمومی اطلاعات¹ یاد می کند. [17]

این نظارتها از سوی مردم آمریکا مداخله در امور خصوصی مردم قلمداد می شود و شکایتهایی هم از DHS شده است بعنوان مثال شکایت مرکز اطلاعات الکترونیک خصوصی² (EPIC) که هنوز در حال پیگیری است. متخصصین این مرکز اعلام کرده اند:

اگر چه کلیه اطلاعات موجود در شبکههای اجتماعی اعم از اطلاعات شخصی و حساس یک منبع تغذیه بالقوه برای متخصصین مهندسی اجتماعی³ هستند و مهندسين اجتماعی از این شیوه استفاده می کنند بنابراین ایجاد آدرسهای دروغین الکترونیکی⁴ (از سوی مامورین امنیتی برای دسترسی به اطلاعات شخصی مردم یک رفتار بی شرمانه است. ارزیابی های FRPIA⁵ که از زیر مجموعه های وزارت امنیت داخلی است نشان می دهد که به آنها اجازه داده شده است که اقدام به ایجاد آدرسهای الکترونیکی دروغین - وجعل نام و رمز ورود افراد نمایند تا بتوانند حداقل ۳۹۰ کلید واژه مهم⁶ در شبکه های اجتماعی را پایش نمایند: کلماتی نظیر:

illegal immigrants, drill, infection, strain, outbreak, virus, recovery, deaths, collapse, human to animal, Trojan..... [18]

در زیر مجموعه تشکیلات مدیریت بحران در ایالات متحده آمریکا نام FEMA شناخته شده ترین نام است و یکی از ادارات تابعه FEMA دستورالعملی را در ماه مار س ۲۰۱۰ منتشر کرده با نام " حفظ حریم خصوصی و امنیتی در شبکه های اجتماعی"⁷ که در آن

⁸ Social security number-

⁹ -DHS social media policy for employees.

¹⁰ -Lewis shepherd, a former senior technology officer at the defense intelligence Agency.

¹¹ Anti western propaganda-

¹² Michael Wertheimer-

¹³ Director of national intelligence for analysis-

¹ Public source information-

² The electronic privacy information center-

³ Social engineers-

⁴ Sock puppet accounts-

⁵ - Federal Register and Privacy Impact Assessments

⁶ Hot key words-

⁷ -security and privacy in social networking sites



مردم با تبلیغات سیاسی و فرهنگی است که تحت عنوان کاربرد شبکه‌ها بعنوان ماشین تبلیغاتی (propaganda machine) شناخته می‌شود. و کاربرد دوم جمع آوری اطلاعات راجع به مدیران و نخبگان کشور است. که در هر دو مورد دارای جنبه امنیتی است. در مهندسی اجتماعی تلاش می‌شود مخاطب را با ترفندهای روانشناسانه و بهره برداری از نیاز انسانها به اعتماد کردن ترغیب کنند که اطلاعاتی خاص را در اختیار طرف مقابل قرار دهد و در شبکه‌های اجتماعی همین احساس نیاز به اعتماد کردن به دوستان، به صورت کاذب در سطح وسیع ایجاد شده است. و ظاهراً راهی برای تغییر سریع عادات افراد جامعه وجود ندارد و درصد زیادی از جوانان ما به این احساس نیاز پاسخ داده اند. جمله معروفی است که می‌گوید " شما نمی توانید هیچگاه برنده میدان بشوید اگر وارد نبرد(بازی) نشوید". در حال حاضر خواسته یا ناخواسته جمع زیادی از جمعیت جوان کشور وارد این بازی شده اند ولی به ابعاد زمین این بازی و خطرات احتمالی این ورطه آشنایی ندارند. بنابراین اگر با یک برنامه ریزی صحیح متخصصین خود را وارد این عرصه نکنیم شکست خواهیم خورد. لذا پیشنهاد می‌گردد:

ابتدا مسئولین ذیربط استراتژی کلی نظام را در مواجهه با این پدیده مشخص کنند.

بسیاری از کارمندان اداری و پرسنل نظامی تکلیف خود را از نظر مقررات کشور در برابر این موضوع نمی دانند لذا تدوین یک سیاست فراگیر برای پرسنل کشوری و یک سیاست اختصاصی تر برای پرسنل لشکری ضروری است. کما اینکه در کشورهای آمریکا- اسرائیل(بعنوان دشمنان اصلی ج.ا.ایران) در بعضی رده‌های لشکری عضویت در این شبکه‌ها ممنوع شده و در سایر رده‌ها با اسامی غیر واقعی و بدون اشاره به نوع و محل خدمت مجاز است.

آموزش همگانی به جوانانی که مخاطب این شبکه‌ها هستند و منبع اطلاعات داخلی کشور محسوب می‌شوند در رابطه با خطرات شخصی برای خود و خانواده‌شان و همچنین خطرات ملی می‌تواند از مشکلات بیشتر جلوگیری کند .

استفاده شده و می‌شود موضوع انتخابات در ایران¹ (Iranian election) است. [21]

نتیجه‌گیری و پیشنهاد

با توجه به مستندات ذکر شده از ماهیت و عملکرد شبکه‌های اجتماعی و بهره برداری‌های امنیتی دشمنان از این بستر، گسترش روز افزون استفاده از این شبکه‌ها در کشور خطرات فراوانی به همراه دارد. که مهمترین آنها خطر جاسوسی است. در ادبیات فارسی جاسوس تعریف مشخصی دارد: کسی که اخبار و اطلاعات شخص، موسسه و یا کشوری را مخفیانه گردآوری کرده و به شخص، موسسه و یا کشوردیگری اطلاع دهد. [۲]

جاسوسی رایانه‌ای نیز در مجموع قوانین جرائم رایانه‌ای تعریف ذیل را دارد:

هرکس به طور غیرمجاز نسبت به داده‌ای سری در حال انتقال یا ذخیره شده در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود:

دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال در دسترس قرار دادن داده‌ای مذکور برای اشخاص فاقد صلاحیت.

افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها [۳]

اهداف جاسوسی در فضای سایبری نیز تعریف شده است که مهمترین آنها اهداف کشوری با مشخصه‌های ذیل است:

- اهداف کشوری
- کسب اطلاعات امنیتی
- کسب اطلاعات استراتژیک و لجستیک
- بررسی راه‌های ممکن جهت جنگ نرم
- بررسی و تحت کنترل گرفتن امکانات موجود جهت سواستفاده‌های احتمالی
- شناسایی و برقراری ارتباط با نخبگان و مدیران قابل

نفوذ [۴]

با توجه به اینکه موضوع بهره برداری تجاری از اطلاعات کاربران منجمله جهت مصارف تبلیغاتی اینترنتی در ج.ا.ایران موضوعیت ندارد. مهمترین کاربرد این شبکه‌ها در کشور ما شکل دادن به افکار

¹ - Iranian elections



منابع:

۱. مقاله تاریخچه وبلاگ در ایران و جهان. www.aftab.ir.
۲. فرهنگ معین - جلد دو
۳. قانون جرایم رایانه ای - فصل یک مبحث سوم.
۴. آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد <http://cert.um.ac.ir>
- [1] Sarah Granger, "Social Engineering Fundamentals, Part II: Combat Strategies", 2002-01-09
- [2] www.facebook.com/...social-network...control-the-world/253109479
- [3] <http://cima.ned.org/publications/social-media-arab-world-leading-uprisings-2011-0>
- [4] http://www.nextgov.com/nextgov/ng_20090415_8127.php
- [5] university of pacific, www.pacific.edu
- [6] <http://www.newmedia.hhs.gov/resources/socialmedia101overview11-2009>
- [7] <http://www.joesblogg.com/2010/03/social-media-usage-statistics-2010/>
- [8] www.socialnetworkingwatch.com
- [9] www.oxyweb.co.uk
- [10] www.oxyweb.co.uk/blog/revision-1/oct/2011
- [11] techcrunch.com
- [12] www.persianblog.com
- [13] news.bbc.co.uk/2/hi/7364091
- [14] http://www.cbsnews.com/8301-501465_162-20019629-501465.html
- [15] <http://www.reuters.com/article/2012/01/11/us-usa-homelandsecurity-websites->
- [16] <http://www.homelandsecuritynewswire.com/dr20120103-dhs-social-media-monitoring-policy-under-fire>
- [17] *ibid.*
- [18] <http://www.networkworld.com/community/blog/privacy-advocates-sue-dhs>
- [19] Emergency Management and response information sharing and analysis center/CIP Bulletin 2-10 March, 23, 2010
- [20] <http://gcn.com/Articles/2009/07/23/Social-networking-media-national-security>.
- [21] *ibid.*

