فصلنامهٔ مطالعات حفاظتی و امنیتی
فصلنامهٔ علمی- ترویجی
سال دوازدهم، شمارهٔ چهل‌ودوم، بهار ۱۳۹۶

تاریخ دریافت: ۱۳۹۵/۱۱/۲۳
تاریخ پذیرش: ۱۳۹۶/۰۲/۲۸

بررسی چگونگی جاسوسی و نفوذ امنیتی دشمن در فضای مجازی

خلیل خسروی[۱]

از صفحهٔ ۱ تا صفحهٔ ۲۰

چکیده

در دورانی که به نام عصر اطلاعات و انفجار اطلاعات مشهور شده، شبکهٔ جهانی اینترنت (فضای رایانه‌ای)، یکی از محورهای جدید فعالیت بشری، ظهور یافته و با سرعتی باورنکردنی در حال درهم‌ریختن تمامی مرزها و چارچوب‌های فیزیکی و غیرفیزیکی در همهٔ جامعه‌ها و نهادها و در همهٔ زمینه‌هاست و به بازیگری مهم و اثرگذار مبدل شده است.

این تحقیق سعی دارد تعریفی از جاسوسی، جاسوسی رایانه‌ای و جاسوسی اینترنتی داشته باشد؛ با تأکید بر تمایزهای آن‌ها و معرفی برخی از روش‌های نوین جاسوسی و چگونگی نفوذ دشمن از راه فضای مجازی. افزون بر آن، به این دلیل که جاسوسی جرم است، جاسوسی رایانه‌ای و اینترنتی هم جزء جرم‌ها شمرده می‌شود و در اصل جرم اجتماعی است. در این مقاله سعی کرده‌ایم، با اشاره به گونه‌های جاسوسی و جاسوسان، به شناخت روش‌ها و هدف‌های جاسوسی دست یابیم و همچنین، با بیان راه‌کارهایی برای مقابله با این‌گونه ابزارهای جاسوسی، به برخی از روش‌های نوین جاسوسی که از راه نرم‌افزارها و بدافزارهای نصب‌شده روی رایانه شکل می‌گیرند بپردازیم.

کلیدواژه‌ها: جاسوسی، جاسوسی رایانه‌ای، جاسوسی اینترنتی، فضای مجازی، فضای سایبری، شبکهٔ اجتماعی.

---

۱. دانشجوی کارشناسی ارشد مدیریت دانشگاه علوم انتظامی امین khalilkhosravi6@gmail.com.

مقدمه

انسان همیشه به داشتن قدرت تمایل دارد و مایل است بـه پیـروزی دسـت یابـد. آگـاهی از وضعیت طرف مقابل یکی از راه‌های کسب قدرت در مبارزه‌ها و رقابت‌ها به‌شمار مـی‌رود. به‌طوراساسی، شناخت به انسان قدرت پیش‌بینی می‌دهد و به دنبال قدرت پیش‌بینـی، انسـان خود را مجهز می‌کند و به موفقیت می‌رسد. در گذشته، وقتی پادشاه کشوری قصـد فـتح و استعمار کشوری دیگر را داشت، برای شناخت مردم آن کشور و افزایش قدرت پیش‌بینـی رفتارهای آنان و آماده‌سازی ارتش خود برای رویارویی با آن‌ها، اسطوره‌های آن کشـور را مطالعه می‌کرد. امروزه این شناخت به همان نیت، ولی با ابزار و راه‌های متفاوت، به شیوه‌ای مجرمانه و با استفاده از فنّاوری روز دنیا، بیشتر در فضای مجازی انجام می‌شود.

امروزه فراگیری اینترنت و فنّاوری‌های جدید ارتباطی و اطلاعاتی موجب ظهور فضـای مجازی در کنار جهان واقعی شده و در نتیجه، معادله‌ها و الگوهای ارتباطات سنتی، تولیـد، انتقال و مصرف اطلاعات را بر هـم زده و موجـب تغییرهـایی در آن‌هـا شـده اسـت. چنـین فضایی که با عنوان واقعیت مجازی یکپارچه در نظـر گرفتـه مـی‌شـود دارای ویژگـی‌هـایی همچون بی‌مکانی، فرازمانی، صنعتی‌بودن محض، محدودنشدن بـه قـوانین مـدنی متکـی بـر دولت‌ـ ملت‌ها، برخورداری از معرفت‌شناسی تغییرشـکل‌یافتهٔ پسـامدرن، دردسـترس‌بـودن هم‌زمان، برخورداری از فضاهای فرهنگی، اعتقادی، اقتصادی، سیاسی و نیز آزادی هویـت بدنی و جنسی جدید اسـت. شـبکه‌هـای اجتمـاعی مجـازی امـروزه نقـش بسـیار مهمـی در پدیدآوردن این فضای مجازی دارند و از خلال همین واقعیت‌هـای مجـازی، ممکـن اسـت آسیب‌های روانی و سیاسی و امنیتی بسیار گسترده‌ای برای جامعه‌ها به‌وجود آورند.

بیان مسئله: نوآوری‌های فنّاورانـه تمـامی قلمـروی زنـدگی بشـری را دگرگـون مـی‌کننـد؛ هرچند، با توجه به نوع فنّاوری، سـرعت تحـول و گسـترش تأثیرگـذاری فنّـاوری متفـاوت خواهد بود. در این میان، انقلاب اطلاعات در دههٔ ۱۹۷۰ که گردآوری، ذخیره و پردازش، انتقال و انتشار اطلاعات را به‌طور چشمگیری تغییر داد، به‌سرعت فعالیت‌هـای انسـانی را در تمامی پهنه‌ها دگرگون کرد. گستره و ژرفای تأثیرگذاری این انقلاب با پیدایش اینترنـت و رایانه‌های شخصی افزایش یافت.

این دو تحول کاربستِ فنّاوری‌های اطلاعات و ارتباطات را، در زمینه‌های نظامی و سیاسی و اقتصادی، از طریق کنشگران دولتی و غیردولتی امکان‌پذیر کرد. روند شتابان گسترش و پراکندگی فنّاوری‌های اطلاعات و ارتباطات جهان را در بستر بافت پسابین‌المللی یا پساوستفالیایی[۱] قرار داده است. این وضعیت بر تمامی جنبه‌های حیات بین‌المللی سایه افکنده و تمامی سطوح فردی، فراملی، ملی، منطقه‌ای و بین‌المللی را درنوردیده است.

اما مسئله اینجاست که کشورها، به‌ویژه کشورهای ابرقدرت، در زمینهٔ کسب اطلاعات مورد نیاز با سرعت بالا برای پیشی‌جستن از کشورهای هم‌تراز خود و دیگر کشورهای دنیا، از جمله کشورهایی که با آن‌ها دشمنی داشتند و در حال جنگ بودند، از چه ابزاری باید استفاده می‌کردند؟ بنابراین، برای دستیابی سریع به این اطلاعات، نیازمند جاسوسی به شیوه‌های متفاوت بودند؛ به‌ویژه، جاسوسی در فضای مجازی با استفاده از فنّاوری‌های جدید و به‌روز. به همین سبب، به فکر ساخت و استفاده از ابزارهای جاسوسی نوین افتادند و در این بین، از روش‌های متنوعی برای رسیدن به هدف‌های خود استفاده کردند که به آن «جاسوسی نوین» گفته می‌شود (ماه‌پیشانیان، ۸۴).

به‌راستی دلیل این امر چیست؟ چرا باید رفتار آدمی در دنیای اینترنت نیز مورد نظارت و واپایش باشد؟

اهمیت و ضرورت تحقیق: اساس ارتباطات در سامانه‌های فرماندهی و واپایش بر هیچ‌کس پوشیده نیست و امنیت اطلاعات بسیار ضروری است. جاسوسی در اصل به‌منظور شناسایی دشمن انجام می‌شود؛ به بیان دیگر، گردآوری اطلاعات پنهانی با استفاده از ترفند و فریب را «جاسوسی» گویند. به این علت که گردآوری اطلاعات بر کسی پوشیده نیست، جاسوسی یکی از مباحث متداول است که بیشتر جامعه‌های نظامی، غیرنظامی و سامانه‌های فرماندهی در آن درگیرند. چون امنیت زیرساخت‌ها و سامانه‌ها در گسترهٔ حفظ اطلاعات مهم است، ابزارهای نوین گردآوری اطلاعات در فضای اینترنتی، مراکز واپایش اطلاعات

---

۱. post Westphalian: دورانی که دولت دچار فرسایش شده و نقش آن کمرنگ شده است. دولت، به‌اجبار، باید به بازیگران جدید و غیردولتی اهمیت بدهد و اینجا نقش بازیگرانی که تا دیروز حاشیه‌ای بودند آشکار می‌شود.

و داده‌های اینترنتی، نرم‌افزارهای رایانه‌ای و بدافزارهای جاسوسی، به‌دلیل شناخت و انجام‌دادن اقدام‌های مقابله‌ای در مقابل برون‌رفت اطلاعات به‌دست دشمنان قسم‌خورده، موضوع‌هایی بسیار مهم‌اند.

هدف‌های تحقیق

هدف اصلی: هدف اصلی مقاله بررسی چگونگی جاسوسی و نفوذ امنیتی دشمن در فضای مجازی است.

هدف‌های فرعی

۱. شناسایی ابزارهای جاسوسی نوین؛
۲. شناسایی روش‌های مقابله با جاسوسی جدید؛
۳. شناسایی هدف‌ها، روش‌ها و راهنمایی‌های امنیتی مقابله با نرم‌افزارهای جاسوسی.

پرسش‌های تحقیق

پرسش اصلی: روش‌های جاسوسی نوین و نفوذ امنیتی دشمن در فضای مجازی چیست؟

پرسش‌های فرعی:

۱. ابزارهای نوین جاسوسی کدام‌اند؟
۲. روش‌های مقابله با جاسوسی نوین چیست؟
۳. هدف‌ها، روش‌ها و نرم‌افزارهای جاسوسی چیستند؟

مبانی نظری: تعریف جاسوسی رایانه‌ای و جاسوسی اینترنتی: اساس پیدایش هک، جاسوسیِ اینترنتی نیست و بسیاری از هکرها هم با انگیزه‌های «تقویت ایمنی داده‌ها، غلبه بر شبکه‌های ایمنی، لذّت‌بردن از نفوذ به بانک‌های مهم داده و مطرح‌شدن بین دوستان یا در رسانه‌ها» (زیبر، ۱۳۸۳: ۴۶) و «گرایش شدید به یادگیری شیوهٔ کار رایانه، یافتن راهی برای ورود مخفیانه به آن و پیداکردن حفره‌های امنیتی سامانه‌ها، هیجان خواندن اطلاعاتی که می‌دانند اجازهٔ دیدن آن‌ها را ندارند یا انجام‌دادن کاری که می‌دانند قانونی نیست» ناخواسته در این مسیر قرار گرفته‌اند (کریم‌بیگی، ۱۳۸۴).

اما آنچه در مسائل حقوقی جاسوسی سبب خلأ قانون شده این است که جاسوسی جزء آن دسته از جرم‌هایی است که وسایل در ارتکاب آن شرط نیست.

فضای مجازی (سایبری): به رایانه‌های متصل به یکدیگر، سرورها، سوئیچ‌ها و کابل‌ها که زیرساخت‌های مهم با آن‌ها کار می‌کنند تا فضایی برای تولید و تبادل مجازی اطلاعات صورت گیرد «فضای مجازی» می‌گوییم. لازم به یادآوری است که پیشوند «سایبر»[1] (شبکه) از واژهٔ «سایبرنتیکز»[2] مشتق شده است؛ یعنی دانش سامانه‌های واپایش و ارتباطات در حیوان‌ها و دستگاه‌ها. خود واژهٔ «سایبرنتیکز» از واژهٔ یونانی «کابرنتز»[3]، به‌معنای «سکان‌دار» گرفته شده است. ویلیام گیبسون[4]، نویسندهٔ آمریکایی داستان‌های علمی‌ـ تخیلی، در اثر مشهور خود به نام *نورومانسر*[5]، عبارت «فضای شبکه‌ای»[6] را برای نخستین‌بار به‌کار برد.

شبکه‌های اجتماعی: به مجموعه‌ای از افراد، که با یکدیگر ارتباط گروهی دارند و مواردی مانند اطلاعات، نیازمندی‌ها، فعالیت‌ها و افکار خود را به اشتراک بگذارند «شبکه‌های اجتماعی» می‌گویند. شبکه‌های اجتماعی را می‌توان به دو دستهٔ «شبکه‌های مجازی» و «شبکه‌های غیرمجازی» تقسیم کرد. شبکهٔ اجتماعی مجازی یا شبکهٔ اجتماعی اینترنتی وب‌گاه یا مجموعه‌ای از وب‌گاه‌هایی است که به کاربران امکان می‌دهد علاقه‌مندی‌ها، افکار و فعالیت‌های خود را با یکدیگر به اشتراک بگذارند؛ به عبارت دیگر، شبکه‌های اجتماعی پایگاه‌هایی‌اند که، با استفاده از موتور جستجوگر و افزودن امکاناتی مانند گفتگوی برخط، پیام‌رسانی الکترونیک، انتقال تصویر و صدا و مانند آن، امکان ارتباط بیشتر کاربران را در قالب شبکه‌ای از روابط فردی و گروهی فراهم می‌آورند ، وبلاگ‌ها، فیس‌بوک، توییتر، یوتیوب و پادکست از جملهٔ شبکه‌های اجتماعی مجازی‌اند (ماه‌پیشانیان، ۱۳۸۴).

---

1. Cyber
2. cybernetics
3. Carbents
4. William Gibson
5. *Neuromancer* (1984)
6. Cyberspace

تاریخچهٔ استفاده از جاسوس‌افزار: واژهٔ «جاسوس‌افزار» نخستین‌بار در ۱۶ اکتبر ۱۹۹۵، در متنی درمورد الگوی تجارتی مایکروسافت، به‌کار رفت. در سال ۲۰۰۰ گریگور فرند[1]، در توصیف دیوار آتش[2] شخصی خود به نام «زون آلارم»[3]، از واژهٔ «جاسوس‌افزار» استفاده کرد. اما کاربرد رسمی از این واژه پس از سال ۲۰۰۱ بود؛ زمانی که استیو گیبسون[4]، رئیس رئیس مرکز تحقیقات «گیبسون»، متوجه نصب نرم‌افزاری تبلیغاتی روی رایانهٔ خود شد که اطلاعات شخصی او را برای فرد دیگری ارسال می‌کرد. به همین دلیل، وی برنامه‌ای ضدجاسوسی طراحی کرد و آن را «اوپت اوت[5]» نامید.

انواع جاسوسی

جاسوسی رایانه‌ای: رایج‌ترین راه جاسوسی رایانه‌ای رونوشت‌کردن پرونده‌های داده است؛ به‌ویژه در زمینهٔ برنامه‌هایی که به تعداد انبوه تولید می‌شوند و به فروش می‌رسند.

نوع دیگر جاسوسی رایانه‌ای «جاسوسی سنتی» است که آن هم به دو دستهٔ «جاسوسی شخصی سنتی» و «جاسوسی فنی سنتی» تقسیم می‌شود.

جاسوسی شخصی سنتی: روش‌های این نوع جاسوسی عبارت‌اند از «رشوه‌دادن به کارمندان یا باج‌گیری از آن‌ها؛ فرستادن مأمور، در قالب کارمند تازه‌وارد، برای دوره‌های کوتاه کاری (این روش به 'سلام‌ـ خداحافظ' معروف است)؛ یا از راه مصاحبه با کارمندان شرکت مورد نظر که در جستجوی کار جدید به سراغ آگهی‌های دروغین می‌آیند و در ضمن مصاحبه وضعیت فعلی کارشان را هم توصیف می‌کنند» (زیبر، ۱۳۸۳: ۴۶).

جاسوسی فنی سنتی: روش‌های فنی سنتی به‌دست‌آوردن اطلاعات ذخیره‌شده در رایانه بر مبنای موارد زیر است ۱. سرقت پرونده‌های داده؛ ۲. اتصال کابلی مخفی به رایانهٔ مورد نظر؛ ۳. نصب بخش انتقال‌دهنده در رایانهٔ مورد نظر.

---

1. Gregorferand
2. Firewall
3. ZoneAlarm
4. Steve Gibson
5. Opet ot

جاسوسی اینترنتی: نوع دیگری از جاسوسی است که خود گونه‌ها و شیوه‌های متفاوتی دارد.

- معرفی برنامه‌هایی که از راه نصب نرم‌افزارها و یا هنگام گردش افراد در محیط وب وارد رایانهٔ شخصی آن‌ها می‌شوند و تا زمان اتصال کاربر به شبکهٔ جهانی، اطلاعاتی را که روی حافظهٔ اصلی رایانهٔ او ذخیره شده است برای پایگاه‌های مطلوب خویش می‌فرستند (افراسیابی، ۱۳۸۳).
- بررسی رایانامه‌های شخصی و سازمانی
- «گزارش عملکرد «وب‌گردیِ» کاربران و سرویس‌دهی عرضه‌کنندگان خدمات اینترنتی به شرکت‌ها و سازمان‌های ذی‌نفع» (افراسیابی، ۱۳۸۳).

تفکیک گونه‌های جاسوسی رایانه‌ای بدین‌شکل است:

انواع جاسوسی	**رایانه‌ای**	رونوشت‌کردن پرونده‌ها
		جاسوسی سنتی (شخصی و فنی)
		برداشت از راه بسامد
		استفاده از شبکه‌های مخابراتی
	اینترنتی	بررسی رایانامه‌های شخصی
		مشاهدهٔ دقیق عملکرد کاربران (وب‌گردی)
		نصب نرم‌افزار

آشنایی با نرم‌افزارهای جاسوسی، هدف‌ها، روش‌ها و راهنمایی‌های امنیتی مقابله با آن‌ها

نرم‌افزارهای PC رُبا: این نرم‌افزارها، بدون اطلاع شما، پیوندی از وب‌گاه‌های خود را در فاوریتس[1] قرار می‌دهند. این میانبرها باعث می‌شوند که بسیاری افراد اتفاقی از وب‌گاه آن‌ها دیدن کنند و بدین‌ترتیب، آمار بازدید وب‌گاهشان بالا می‌رود.

1 .favorites

این اتفاق به آن‌ها امکان دریافت مبلغ بیشتری را بابت تبلیغات در وب‌گاهشان می‌دهد که هزینهٔ پرداخت‌شدهٔ آن همان زمان و پهنای باندی است که از شما گرفته می‌شود. اما گاه تنها راه خلاص شدن از این پیوندهای مزاحم پاک‌کردن آن‌ها از درون حافظه[1] است. به هر حال، ممکن است این نرم‌افزار جاسوسی طوری طراحی شده باشد که با هربار راه‌اندازی رایانه، خود را درون حافظه قرار دهد. تنها راه‌حل پیش پای شما برای کشتن این نوع جاسوس متجاوز بازآرایی داده‌های[2] حافظهٔ اصلی رایانه یا استفاده از برنامهٔ ضدجاسوسیِ بسیار قدرتمند است.

نرم‌افزارهای جاسوسی مرورگرربا: برخی افراد رایانهٔ شما را برای استفادهٔ خود در دست می‌گیرند. کاربران نرم‌افزارهای جاسوسی می‌توانند اتصال شما را برای ارسال هرزنامه‌هایشان، از راه سرویس‌دهندهٔ اینترنت شما، بربایند؛ بدین‌معنا که هرزنامه‌ساز انگل ممکن است هزاران رایانامه به صورت هرزنامه را از طریق شما ارسال کند. کاربرانی با دسترسی‌های پرسرعت و ISP اتصال رایانه به اینترنت به‌طورمعمول هدف این نوع کاربران قرار می‌گیرند. بیشتر قربانیان متوجه نمی‌شوند که از اعتبار آن‌ها سوءاستفاده شده است، تا زمانی که خدمات اینترنت، به علت شکایت علیه هرزنامه‌ها، اتصالشان را قطع کند.
نرم‌افزارهای جاسوسی مودم‌ربا: اگر برای اتصال به اینترنت از مودم و خط تلفن استفاده می‌کنید، «جاسوس» ممکن است قادر باشد شماره‌گیر برخطی برای برقراری اتصال جدید اینترنت روی رایانهٔ شما نصب کند. این اتصال ممکن است از دستهٔ اتصال‌های راه دور با هزینهٔ بالا باشد؛ هنگامی که، قبض تلفن را دریافت می‌کنید، غافلگیر خواهید شد. این نرم‌افزارهای جاسوسی اغلب درون هرزنامه و رایانامه‌های مربوط به امور جنسی قرار دارند. بازکردن رایانامه می‌تواند به‌صورت سهوی سبب آغاز نصب شماره‌گیر شود. این افراد بدذات، که پی‌گیری‌شان کار آسانی نیست، به این حقیقت اهمیت می‌دهند که شما قبض تلفن را، پیش از اینکه فرصت پیگیری داشته باشید، پرداخت می‌کنید.

---

1. registery
2 . Formating

ویروس‌ها: امروزه همهٔ ما روی سامانه‌های خود با انواع ویروس‌ها روبه‌رو شده‌ایم. برخی از ویروس‌ها به‌شکل بی‌ضرری در رایانهٔ شما کمین کرده‌اند ولی در واقع از سامانهٔ شما سوءاستفاده می‌کنند. برخی ویروس‌ها به‌طورکامل سامانه را به هم می‌ریزند و شما را مجبور به عوض‌کردن سیستم عامل می‌کنند. برخی ویروس‌ها وارد حافظه‌های جانبی می‌شوند و پرونده‌های داخل آن را به‌کلی نابود می‌کنند و یا آن‌ها را مخفی نگاه می‌دارند. این مسئله باعث شده است بسیاری از کاربران فکر کنند که دیگر کار از کار گذشته و تمامی پرونده‌های آن‌ها از بین رفته است ولی در واقع چنین نیست. برخی ویروس‌ها، همان‌طور که گفتیم، پرونده‌های شما را مخفی می‌کنند اما شما می‌توانید آن‌ها را بازگردانید و از مخفی‌شدن خارج کنید ولی متأسفانه امروزه بیشتر کاربران با این نکتهٔ ساده آشنا نیستند.

هدف نرم‌افزارهای جاسوسی: نرم‌افزار جاسوسی عاملی آزاردهنده است که سرعت رایانه را کم می‌کند، حافظهٔ اصلی سامانه را بی‌دلیل پر می‌کند و رایانهٔ شما را به هدفی برای تبلیغ‌کنندگان تبدیل می‌کند. بدون اطلاع شما ممکن است در سامانهٔ شما جاسوسی کند و اطلاعات خصوصی شما را بگیرد.

روش‌ها و راهنمایی‌هایی برای مقابله با نرم‌افزارهای جاسوسی

- بازنکردن صفحه‌های ناشناس وب: هنگام گشت‌وگذار در اینترنت، هیچ‌گاه صفحه‌های ناشناس و تبلیغاتی را که به نوعی شما را به سمت خود جلب می‌کنند تا بتوانند به هدف‌های خود برسند باز نکنید.
- توجه به هشدارهای آنتی‌ویروس‌ها: هنگام کار با سامانه یا اینترنت، به هشدارهای آنتی‌ویروس توجه کنید و آن را مد نظر داشته باشید چون شاید شما بپندارید آنچه آنتی‌ویروس شناسایی کرده مهم نیست ولی، در واقع، خلاف آن درست باشد.
- به‌روزرسانی نرم‌افزارهای ضدویروس: فقط نصب برنامهٔ ضدویروس و داشتن سامانه‌ای بدون ویروس و مقاوم در برابر حملهٔ ویروس‌ها ختم نمی‌شود. هرروزه ویروس‌های جدیدی عرضه می‌شود و در سال‌های اخیر، انتشار سریع کرم‌ها از راه اینترنت میزان ایجاد ویروس‌ها را افزایش داده است. این مسئله، در ترکیب با افزایش دانش عمومی درمورد

مشکلات امنیتی نرم‌افزارها و سیستم‌های عامل، سرعت ایجاد ویروس‌های جدید را افزایش داده است. امروزه برای ایجاد ویروس نیاز به مهارت و تخصص زیادی نیست.

- بیان تعریف واضح و مشخص از این جرم و رسیدن به توافقی بین‌المللی بر سر تعریف از جاسوسی رایانه‌ای و اینترنتی؛
- ایمن‌کردن رایانه‌های اداری و حتی رایانه‌های شخصی با ابزار و نرم‌افزارهای ضدجاسوسی؛
- آموزش کاربران رایانه، حتی در سطحی ابتدایی، برای آگاهی از خطر جاسوسی و آشنایی اولیه با روش‌های آن؛
- تصویب قوانین جزایی برای جرائم رایانه‌ای، همچون جاسوسی رایانه‌ای، و اعلام این قانون‌ها و مصوبه‌ها به همگان.

شبکه‌های اجتماعی و آسیب‌های سیاسی ـ امنیتی: قراردادن اطلاعات حریم خصوصی کاربران در اختیار دولت‌ها و شرکت‌های تجاری همیشه یکی از موضوع‌های بحث‌برانگیز در دامنهٔ اینترنت و به‌ویژه شبکه‌های اجتماعی بوده است. برخی معتقدند این شبکه‌ها، در عمل، مراکز جاسوسی پرزرق‌وبرق آمریکا محسوب می‌شوند. در واقع، آمریکا با کمترین هزینه می‌تواند هم نظرسنجی خوبی از جامعه‌ها داشته باشد و هم مسیر جریان افکار عمومی را زیر نظر بگیرد. جولین آسانژ[1]، بنیانگذار وب‌گاه ویکی‌لیکس[2]، دربارهٔ یکی از شبکه‌های معروف اجتماعی می‌گوید: «فیس‌بوک تنفرآمیزترین ابزار جاسوسی است که تا کنون خلق شده است. هر کس که نام و مشخصات دوستان خود را به این شبکهٔ اجتماعی اضافه می‌کند باید بداند به‌رایگان در خدمت دستگاه‌های اطلاعاتی آمریکاست و این گنجینهٔ اطلاعاتی را برای آن‌ها تکمیل می‌کند» به اعتقاد وی، موضوع این نیست که فیس‌بوک را دستگاه‌های اطلاعاتی آمریکا هدایت می‌کنند؛ نکته این است که این دستگاه‌ها می‌توانند، با روش‌های حقوقی و یا سیاسی، این شبکهٔ اجتماعی را زیر فشار قرار دهند. رویدادهای سیاسی سال‌های اخیر، از انتخاب باراک اوباما به

1. Julian Paul Assange
2. WikiLeaks

رئیس جمهوری آمریکا گرفته تا ناآرامی‌های پس از انتخابات جمهوری اسلامی ایران، همگی کم‌وبیش متأثر از فعالیت‌های کاربران شبکه‌های اجتماعی بوده‌اند. انقلاب‌ها و خیزش‌های اجتماعی در کشورهای عربی، در چند ماه اخیر نیز، نمونه‌ای از کارکردها و آسیب‌های سیاسی این شبکه‌ها را بازنمایی می‌کند (ماه‌پیشانیان، ۱۳۸۴).

جنبش‌های اجتماعی جدید و هویت‌های دگرخواهانه از مهم‌ترین جنبه‌های نرم‌افزاری تهدید امنیت ملی به‌شمار می‌روند. این جنبش‌ها تلاش دارند با فنّاوری‌های ارتباطی جدید و دگرگونی‌های اجتماعی، سیاسی و فرهنگی سازگار شوند. گاه شبکه‌های اجتماعی، در لباس سربازان جدید جنگ نرم به نفع دولت‌های غربی، اقدام‌های خود را به فضای واقعی جامعه نیز سرایت می‌دهند و هماهنگی و سازمان‌دهی تجمع‌های سیاسی و اعتراضی بر ضد دولتِ هدف را برعهده می‌گیرند. بخش عمده‌ای از رخدادهای اعتراض‌آمیز ایران، طی ماه‌های پس از انتخابات ریاست جمهوری دهم، در فضای مجازی ساماندهی شد. پوشش غیرواقعی خبری اغتشاش‌ها و دعوت به تجمع‌های غیرقانونی، توهین و فحاشی، دخالت آشکار برخی سیاست‌مداران و دولت‌مردان غربی در امور داخلی ایران و دامن‌زدن به ناآرامی‌های موجود از نمونه‌های کاربرد شبکه‌های اجتماعی مجازی علیه امنیت کشورمان بوده است. فیس‌بوک نقش مهمی در گردآوری کمک برای معترضان و حمایت از آن‌ها را داشت. همچنین، ایرانیان از توییتر استفاده می‌کردند تا به وب‌نوشت‌ها و صفحه‌های اینترنتی پیوند بدهند که عکس‌ها و ویدیوهای معترضان را دربر داشتند. به گفتهٔ رابرت فایرز[1]، مدیر مرکز برکمن[2]: «ماهیت نامتمرکز ابزارهایی همچون توییتر دراختیارگرفتن آن‌ها را برای دولت مشکل می‌کند زیرا دارای منابع اطلاعاتی بی‌شماری‌اند که مسدودکردن آن‌ها موجب بدنامی و واکنش جمعی در افکار عمومی می‌شود؛ بنابراین، می‌تواند نقش مهمی در سازمان‌دهی به اعتراض‌های جمعی داشته باشد» (ماه‌پیشانیان، ۱۳۸۴).

1. Robert Fires
2. Berkman

در اینجا، به‌اختصار، آسیب‌های سیاسی و امنیتی شبکه‌های اجتماعی را مطرح می‌کنیم:

مهم‌ترین پیامدهای سیاسی فنّاوری‌های ارتباطی ـ اطلاعاتی تضعیف دولت‌های ملی، نشر اطلاعات سیاسی و کاهش مشارکت سیاسی افراد و گروه‌هاست. همچنین واپایش اطلاعات در دوران جدید اهرمِ اصلی قدرت بازیگران جهانی، ملی و محلی است؛ اهرمی که در انقلاب‌های رنگی در اختیار بنیاد سوروس[1] و سازمان‌های غیردولتی و جنبش‌های دانشجویی قرار گرفت و رهبران حزب‌ها و جنبش‌ها بیشترین بهره را از آن بردند. دولت‌های غربی، ماهرانه، با استفاده از امکانات فنّاوری و ارتباطات مانند اینترنت، پایگاه‌های انتقادی را علیه یک دولت سازمان می‌دهند. پیام‌های کوتاه را از طریق تلفن‌های همراه رد و بدل می‌کنند و پی‌درپی قرارهای جدیدی می‌گذارند.

آسیب مهم دیگر رسانه‌های نوین تأثیر در افکار عمومی و بسیج آن است؛ به‌گونه‌ای که از راه این رسانه‌ها گونه‌ای فضای عمومی شکل می‌گیرد و بسیاری افراد، بی‌آنکه یکدیگر را ببینند و تبادل‌نظر داشته باشند، مانند همدیگر فکر می‌کنند و در نتیجه، رفتارشان نیز مانند یکدیگر است؛ بر این اساس، با تولید پیام و شعار و اندیشه، به شیوه‌ای هنری و از طریق تصویر، گرافیک، صدا و موسیقی، تصورها دستکاری و بسیج می‌شوند و سرانجام، فعالیت سیاسی این امکان را می‌یابد که با زندگی روزمره درآمیزد. در این صورت، دیگر مانند گذشته نیاز نیست که برای تبدیل افکار عمومی به نیروی اجتماعی و تغییر اوضاع سیاسی به اهرمی مانند حزب سیاسی پناه برد و اگر این تغییر در افکار عمومی پیدا شود، خود مردم در مواقع مهم تاریخی راه را باز می‌کنند و احتیاجی به اعمال نیرو، فشار و زور از طریق اهرم‌های جدا از مردم نیست (افضلی بروجنی، ۱۳۹۲: ۳۵).

ابزار جاسوسی فیس‌بوک: شبکهٔ اجتماعی فیس‌بوک که بر اساس اسناد موجود رابطهٔ تنگاتنگی با سازمان‌های جاسوسی آمریکا دارد، متهم شده که با استفاده از پرونده‌هایی به نام سوپرکوکیز[2]، تمامی فعالیت‌های برخط کاربران خود را، حتی در زمان حضورنداشتن آن‌ها در این شبکه، ردیابی و مشاهده می‌کند.

---

1. Soros Foundation
2. supercookies

ابزارهای جاسوسی[1]: «ابزارهای جاسوسی» اصطلاحی عمومی است و درمورد نرم‌افزارهایی به‌کار می‌رود که کارهای خاصی، همچون تبلیغات و گردآوری اطلاعات شخصی و تغییردادن تنظیمات رایانه‌ها، انجام می‌دهند و تمامی این کارها بدون اطلاع و اجازهٔ شما صورت می‌گیرد. گاه ابزارهای جاسوسی با نرم‌افزارهای دیگر، که کار تبلیغات را انجام می‌دهند، یا نرم‌افزارهایی که کارها یا اطلاعات مهم شما را واپایش می‌کنند همراه می‌شوند.

شکل دیگری از ابزارهای جاسوسی تغییرهایی را در رایانه‌ها انجام می‌دهد که ممکن است باعث رنجش دارندگان آن‌ها و گاه موجب کاهش سرعت و به‌طورمعمول سبب خرابی رایانه شود؛ مانند:

- تغییر صفحهٔ خانگی[2]؛
- تغییر پیش‌فرض گزینهٔ جستجوی آن‌ها؛
- افزودن اجزای اضافی که شما آن‌ها را نمی‌خواستید.

گونه‌های نرم‌افزارهای جاسوسی: در یک تقسیم‌بندی کلی، این نرم‌افزارها را می‌توان دو دسته کرد:

۱. نرم‌افزارهای جاسوسی خانگی؛
۲. نرم‌افزارهای جاسوسی تجاری.

شناسایی راه‌های نفوذ

- **پنجره‌های پاپ‌آپ**[3]: پنجره‌های کوچکی که به‌هنگام بازدید از وب‌گاه، در برابر کاربر ظاهر می‌شوند و پیام‌های گوناگونی برای فریب اشخاص دارند. در این پنجره‌ها، به‌طورمعمول دکمه‌های متفاوتی مانند «پذیرش»، «لغو» و «بستن» وجود دارد ولی هیچ‌یک از آن‌ها کار اصلی خود را انجام نمی‌دهد و با فشردن هر یک از این دکمه‌ها، جاسوس‌افزار روی سامانه نصب می‌شود.

1. spyware
2. home page
3. pop-up

- **برنامه‌های رایگان اینترنتی:** امروزه بسیاری از کاربران اینترنت، بنا بر نیاز خود، برنامه‌هایی را که به‌رایگان روی اینترنت قرار گرفته بارگیری و نصب می‌کنند. بیشتر صاحبان این برنامه‌ها، در ازای دریافت مبلغی یا با هدف‌های تجاری دیگر، رمز جاسوس‌افزار را در برنامهٔ خود قرار می‌دهند و هنگام نصب آن نرم‌افزار، جاسوس‌افزار نیز روی رایانه قرار می‌گیرد و شروع به کار می‌کند.
- **لوح‌های فشرده و فلش‌ها:** حافظه‌های جانبی جابه‌جاشدنی، مانند لوح فشرده و فلش، به این علت که بین سامانه‌های بسیاری جابه‌جا می‌شوند، دربردارندهٔ برنامه‌های مخرب‌اند.
- **ویروس‌ها:** برخی ویروس‌ها رمزهایی برای نصب جاسوس‌افزار دارند.

نشانه‌های وجود جاسوس‌افزار در رایانه

تشخیص آلوده‌بودن رایانه به جاسوس‌افزار کار سختی نیست. سامانهٔ آلوده نشانه‌های ساده‌ای دارد، از جمله:

- تغییر ناگهانی صفحهٔ خانگی مرورگر؛
- ایجاد نوارابزارهای جدید؛
- ظاهرشدن پی‌درپی پنجره‌های پاپ‌آپ؛
- تغییر نشانی از سوی مرورگر؛
- ایجاد آیکن‌های[1] جدید (نشان‌های تصویری) روی صفحهٔ نمایش؛
- عملکرد کند رایانه؛
- خاموش‌شدن دیوار آتش و ضدویروس.

یک فنّاوری جاسوسی با ظاهر معصومانهٔ اسباب‌بازی: ارتش آمریکا در حال گسترش هواپیماهای جاسوسی مینیاتوری و کوچکی است که شبیه به اسباب‌بازی و در اندازهٔ پرندگان و حتی حشرات‌اند. به نظر می‌رسد این ابزارها اسباب‌بازی‌های کوچک قدیمی

1. icon

باشند که از انباری بیرون آمده‌اند. اما این دستگاه‌های به‌ظاهر معصوم در واقع پیشرفته‌ترین سازوبرگ جاسوسی ارتش آمریکا شمرده می‌شوند.

مأموریت آزمایشگاه نیروی هوایی این پایگاه نظامی، گسترش سوسک‌های جاسوس[۱] است که بتوانند مهاجمان را، در محیط‌های شهری پیچیده که دخالت نیروهای نظامی ممکن است منجر به تشویش عمومی شود، ردیابی و پیدا کنند.

در بدن این سوسک‌ها تراشه‌ای کاشته شده بود که، با ارسال تحریکاتی به مغز، می‌شد فرود و پرواز آن‌ها را رصد کرد.

در این آزمایش‌ها، محققان دانشگاه کالیفرنیا در برکلی از سه نوع سوسک بزرگ کامرونی استفاده کردند که کوچک‌ترین آن‌ها دو سانتیمتر و بزرگ‌ترین آن‌ها بیست سانتیمتر طول داشت.

آیفون؛ ابزار جدید جاسوسی آمریکا علیه ایران: علاقهٔ ایرانی‌ها به فنّاوری‌های نوین ارتباطی سبب شده آمریکا، در جریان تلاش خود برای ضربه‌زدن به دولت ایران، از این راه وارد شود.

این علاقه سبب شد بخش فارسی «صدای آمریکا»[۲] به‌سرعت بدین‌مسئله پی ببرد و با عرضهٔ امکاناتی ویژهٔ گوشی‌های آیفون و همچنین گوشی‌های جدید اندروید/ گوگل، این امکان را به صاحبان این نوع گوشی‌ها در ایران بدهد تا تصویرهای خود را مستقیم از گوشی همراهشان برای این شبکه بفرستند؛ بدین‌ترتیب، هرکس دارای این گوشی‌ها باشد تبدیل به خبرنگار آن‌ها می‌شود.

---

۱. ربات‌های زنده که به‌اختصار MAV خوانده می‌شوند.

2. VOA

راه‌کارهای پیشنهادی مدیریت شبکه‌های اجتماعی مجازی (از دیدگاه امور امنیتی ـ انتظامی)

- شبکه‌های اجتماعی و فعالیت آن‌ها باید به‌طور منظم و همیشگی زیر نظر گرفته و پایش شود؛
- اطلاعات منتشرشده در سطح شبکه‌های اجتماعی به صورت منظم گردآوری و بررسی و مستندسازی شود؛
- آموزش و اطلاع‌رسانی اثربخش به کاربران شبکه‌های اجتماعی صورت گیرد؛
- به رشد و گسترش (کمّی و کیفی) امور مطالعاتی و پژوهشی در زمینهٔ فعالیت‌های شبکه‌های اجتماعی کمک شود؛
- داده‌کاوی (طراحی و ایجاد پایگاه برای داده‌های مناسب) گسترش یابد؛
- عملیات روانی و ضد عملیات روانی مناسب در سطح شبکه‌های اجتماعی اجرا شود؛
- امنیت اطلاعات و ارتباطات در فضای مجازی گسترش یابد؛
- سازوبرگ و رایانه‌هایی که برای کار در فضای مجازی استفاده می‌شوند به هیچ عنوان نباید به شبکه، سازوبرگ و بسترهای درون‌سازمانی مانند نودهای شبکهٔ اینترانت ناجا و رایانه‌های درون‌سازمانی متصل شوند. برای هرگونه اقدام، باید از رایانه‌ها و سازوبرگ منفرد و قابل اطمینان استفاده شود؛
- تمامی سازوبرگ‌های شنود و یا تصویربرداری، مانند صدابر و وب‌کم (دوربین‌های اینترنتی)[1] (داخلی یا اکسترنال)، باید در مواقع غیرضروری از روی سامانه‌های مورد استفاده برای فعالیت در فضای مجازی قطع شوند؛
- نرم‌افزارهای قوی و مناسب، برای مقابله با بدافزارها و ویروس‌ها و ازبین‌بردن آن‌ها، و همچنین دیوار آتش قوی و مناسب روی رایانه‌ها و سازوبرگ نصب و به‌موقع به‌روزرسانی شود؛
- به هیچ عنوان از اطلاعات واقعی و حقیقی، عکس و تصویر واقعی و همچنین رایانامه‌های اصلی برای ثبت‌نام در وب‌گاه‌ها، وبلاگ‌ها و شبکه‌های اجتماعی، استفاده نشود. هرگونه ثبت اطلاعات و یا مشخصات با عناوین و تصاویر غیرواقعی باشد.

1. Webcam

- برای اینکه سرویس‌های حریف موفق به شناسایی نشوند، باید رایانامه‌ها و انگاره‌های ایجادشده در شبکه‌های اجتماعی، شماره تلفن‌های همراه یا ثابت، نشانی‌های الکترونیکی و هرگونه نشانی و شمارهٔ مورد استفاده در فضای مجازی، در فواصل زمانی کوتاه تغییر داده شود؛ بدین‌صورت که هر نشانی و یا شماره فقط مدت کوتاهی به‌کار رود. همچنین، به‌منظور امکان موشکافی ایستگاه‌های اینترنتی مورد استفاده، از ایستگاه‌های متفاوتی استفاده شود؛
- برخی از وب‌گاه‌ها و شبکه‌های اجتماعی، به‌منظور هویت‌شناسی دقیق‌تر، رمزهای عبور را به تلفن‌های همراه ارسال می‌کنند. بهتر است در این زمینه نیز تمهیداتی اندیشیده شود و با هماهنگی درگاه‌های مربوط، شماره‌هایی برای این منظور در نظر گرفته شود؛
- حضور همیشگی در فضای مجازی و استفادهٔ پی‌درپی از اینترنت، به‌خودی‌خود، باعث بروز آسیب‌هایی می‌شود؛ آسیب‌های جسمی، روحی و روانی، فکری، اخلاقی، اعتقادی و حتی سیاسی و امنیتی. افرادی که از این فضا زیاد استفاده می‌کنند از چنین آسیب‌هایی در امان نیستند و ممکن است، به‌علت فعالیت زیاد و مستمر، دچار نوعی یکنواختی شوند و به عقیده‌ای، اصول و معیارهای موجود در فضای مجازی برای آن‌ها عادی و باورپذیر شود؛ بنابراین، مبادی مربوط باید تدابیر و راه‌کارهای پیشگیرانه و اصولی را در این زمینه در نظر بگیرند؛
- از هرگونه استفاده از سازوبرگ و سخت‌افزارها، نرم‌افزارها و سامانه‌هایی که درگاه‌های سازمانی تأیید نکرده‌اند ــ مانند موارد اهدایی و کشف‌شده، خریداری‌شده از شرکت‌ها و افراد بدون صلاحیت و خارج از چرخهٔ سازمانی ــ خودداری شود؛
- رعایت اصل حیطه‌بندی باید همیشه مدنظر یکایک کارکنان قرار گیرد؛ بدین‌معنا که هر یک از کارکنان، با توجه به دسترسی‌های تعیین‌شده، شناسه و گذرواژه‌های واگذارشده، وظایف مشخص‌شده و میزان اطلاعات در اختیار گذاشته‌شده، فعالیت کنند و در حفظ و نگهداری آن‌ها طبق مقررات بکوشند و از واگذاری دسترسی، اختیارات و اطلاعات خود به افراد غیرمجاز خودداری کنند؛
- رایانه‌ها و سازوبرگ مورد استفاده در فضای مجازی، در سه سطح سخت‌افزار و سیستم عامل و برنامه‌ها، باید از لحاظ امنیتی و بستن راه‌های نفوذ و رفع خطاهای[1] پیکربندی امن شود؛

1. bugs

- داده‌های حساس به هیچ عنوان در ابزارهای متصل به فضای مجازی و شبکه نگهداری نشوند. هر نوع اطلاعات الکترونیکی دریافت‌شده و داده‌ها باید در محل مناسب و ایزوله نگهداری شوند و پروندهٔ موجود در ابزارهای متصل به فضای مجازی، با استفاده از نرم‌افزارهای مناسب، از بین برود؛
- پرونده‌ها و پیام‌های ناشناس در فضای مجازی را اصلاً نباید باز کرد (استرکی، ۱۳۹۱).

نتیجه‌گیری

جاسوسی رایانه‌ای یکی از جرم‌های رایانه‌ای با قدمتی دیرینه است و در امتداد تلاش‌های نظامی و سیاسی، برای کسب آگاهی از طرف مقابل به هنگام جنگ یا هر رقابت دیگری، پدید آمده است. اما با راه‌اندازی شبکهٔ اینترنت، این جرم هم ماهیتی متناسب با قالب فضای مجازی یافت و با تغییر و پیدایش روش‌های جدید که نتیجهٔ فضای مجازی و ویژگی‌های آن بود، به گونهٔ جدیدی از جاسوسی، یعنی جاسوسی اینترنتی یا مجازی، تبدیل شد. به‌طوراساسی، باید بین جاسوسی رایانه‌ای و جاسوسی اینترنتی تمایز قائل شد، زیرا هم در ماهیت و هم از لحاظ روش‌های مورد استفاده، با هم متفاوت‌اند.

در جاسوسی رایانه‌ای، به‌طورمعمول از روش‌هایی مانند رونوشت‌کردن پرونده‌ها، جاسوسی سنتی، برداشت از طریق بسامد و استفاده از سامانه‌های مخابراتی استفاده می‌شود و در جاسوسی اینترنتی، نصب نرم‌افزارهایی که در مدت اتصال کاربر به شبکه روی رایانهٔ او (بااجازه یا بی‌اجازه) نصب می‌شود، بررسی رایانامه‌های شخصی با هک‌کردن رمزهای آن، مشاهدهٔ دقیق عملکرد کاربران و خدمات‌دهندگان اینترنت به‌کار می‌رود. تفاوت اصلی و بنیادی این دو شکل جاسوسی در این است که جاسوسی رایانه‌ای نیاز به استخدام مزدور دارد و بدون عنصر میانجی نمی‌توان اطلاعات به‌دست آورد و به‌یقین هزینه‌های مالی هم دربر دارد.

به هر حال، در هر دو گونهٔ جاسوسی (اینترنتی و رایانه‌ای)، هدف دستیابی به اطلاعات نظامی، سیاسی و حتی شناخت ویژگی‌های فرهنگی‌ـاجتماعی، با هدف‌های سیاسی‌ـامنیتی است؛ بنابراین، می‌توان گفت جاسوسی به روش‌های یادشده، بی‌اخلاقی در دنیای مجازی به‌شمار می‌رود.

منابع:

افراسیابی، محمدصادق (۱۳۸۳)، «اینترنت آن‌لاین‌ترین جاسوس دنیا» شبکه‌های اطلاع‌رسانی جهانی، سروش، شمارهٔ ۱۲۰۴، صص ۵۲-۵۴.

افضلی بروجنی، گلشن‌السادات، و دیگران (۱۳۹۲)، «چالش‌های امنیتی و راه‌کارهای مقابله با آن در شبکه‌های اجتماعی»، *مجموعه مقالات همایش تخصصی بررسی ابعاد شبکه‌های اجتماعی*، تهران: جهاد دانشگاهی.

زیبر، اولریش (۱۳۸۳)، *جرائم رایانه‌ای*، ترجمهٔ محمدعلی نوری و دیگران، تهران: گنج دانش.

کریم بیگی، آرش (۱۳۸۴)، *امنیت اطلاعات*، یزد: آفتاب.

کوردنر، گری دبلیو (۱۳۹۱)، *مدیریت پلیس*، ترجمهٔ اکبر استرکی، تهران: زرد.

ماه‌پیشانیان، مهسا (۱۳۸۴)، «آیا ایدهٔ سنتی امنیت نیاز به بازنگری دارد»، *راهبرد*، شمارهٔ ۳۵، صص ۱۲۳-۱۸۳.

مطالعهٔ بیشتر:

اشرف، احمد (۱۳۲۵)، *کژرفتاری مسائل انسانی و آسیب‌شناسی اجتماعی*، تهران: انتشارات آموزشگاه عالی خدمات اجتماعی.

افضلی، هادی، و دیگران، «جاسوسی دیجیتال مدرن در سامانه‌های فرماندهی و کنترل».

آیکاو، دیوید جی (۱۳۸۳)، *راه‌کارهای پیشگیری و مقابله با جرائم رایانه‌ای*، ترجمهٔ اکبر استرکی و دیگران، تهران: دانشگاه علوم انتظامی معاونت پژوهش.

ریتزر، جورج (۱۳۸۵)، *نظریه‌های جامعه‌شناسی*، ترجمهٔ احمدرضا غروی‌زاد، تهران: جهاد دانشگاهی.

کوثری، مسعود (۱۳۸۶-۱۳۸۵)، *نظریه‌های آنومی اجتماعی*، تهران: دانشگاه علوم بهزیستی و توانبخشی دانشگاه تهران.

نورمحمدی، (۱۳۹۲)، *تهدیدات سایبرتروریسم علیه امنیت ملی ایران*.

http//vag.ir/public.

http//ictna.ir (08-11-2007).

http//amoltek.com (08-11-2007).

http//masihm.com (08-11-200۷).

http//hamshahrionline.ir (14-11-2007).