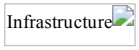
پشت‌پرده سازمان اطلاعاتی – نظامی «وایبر»

*** مقدمه**

با تحقق عصر ارتباطات در جهان، بسیاری از مسائل دست‌خوش تغییر شد. از جمله مواردی که متحول شد، شیوه و بستر ارتباط میان افراد بود. در این مرحله، بیشترِ ارتباطات از حالت حضوری و فیزیکی به صورت سایبری تبدیل شدند و این امکان نیز از طریق ابزارهای سایبرنتیک مثل موبایل، تلفن، پیامک و ... فراهم شد. اما از سال ۲۰۰۴ با راه‌اندازی اولین شبکه اجتماعی مهم در جهان یعنی فیسبوک[۱]، این ارتباطات شکل جدیدی به خود گرفتند. تقریبا از سال ۲۰۱۰ با ورود اولین نسل پیام‌رسان‌های فوری موبایلی، همان سطح ارتباطی که قبلا در شبکه‌های اجتماعی وجود داشت، با این نرم‌افزارها پرشتاب‌تر، پیچیده‌تر، آمیخته‌تر و بسیار لحظه‌ای‌تر شد. ایرانیان یکی از کاربران اصلی فضای سایبر هستند، خصوصا در رده سنی ۱۲ الی ۳۰ سال که بیشترین استفاده از تکنولوژی سایبری را دارند.

مسئله اینجاست که هر تکنولوژی غربی در زمینه سایبر، یک بن‌مایه اطلاعاتی، نظامی، امنیتی در پس پرده دارا است؛ اما متأسفانه شناخته نمی‌شود و فقط به عنوان یک تکنولوژی ارتباطی به بقیه کشورها از جمله ایران وارد می‌گردد. در داخل نیز نسبت به آن نه توجیه امنیتی صورت می‌گیرد نه خطرات اطلاعاتی آن به کاربران اخطار داده می‌شود. در نتیجه جامعه نسبت به آن آگاه نمی‌شود و از طرف دیگر پیوست فرهنگی لازم نیز برای آن تهیه نمی‌گردد. لذا مسئولین مربوطه زمانی بیدار می‌شوند که جامعه درگیر آن تکنولوژی جدید شده و خطراتش به جای اینکه از پیش شناخته شود، کاملا عینی و آشکار گشته و ابتلا جامعه به آن مشاهده می‌شود. از مواردی که متأسفانه اینگونه شناخته شد، پیام‌رسان‌های فوری بود. شهرت این نرم‌افزارها در ایران از طریق وی‌چت[۲] حاصل شد. در حال حاضر رایج‌ترین این پیام‌رسان‌ها در ایران وایبر[۳] است.



(http://fa.nsainfo.ir/wp-content/uploads/Infrastructure.jpg)

*** نقش توان فنّی در اشراف اطلاعاتی سازمان‌های سایبری**

لازم است پیش از شفاف‌سازی سازمان امنیتی وایبر، مبحثی کلان پیرامون ویژگی‌های فنی و مخابراتی شبکه‌های پیام‌رسان فوری ارائه شود.

امروزه بیشتر افراد در ایران از تلفن همراه استفاده می‌کنند و توسط آن حدأقل برای برقراری تماس و ارسال پیام متنی بهره می‌برند. آنچه مهم است اینست که وقتی از یک مبدأ به مقصدی خاص میان دو کاربر پیامی ارسال شود، توان پوشش آنتن و وجود زیرساخت‌های مخابراتی که بتوانند این ارتباط را وصل کنند و پشتیبانی نمایند بسیار مهم است؛ چرا که اگر این زیرساخت‌ها نباشند، این ارتباط برقرار نخواهد شد.

بعنوان مثال اگر یکی از اپراتورهای تلفن همراه در ایران مد نظر قرار گیرد؛ مشخص است که میلیاردها تومان هزینه تاسیسات سخت‌افزاری آن است. علاوه بر آن، حجم گسترده‌ای پرسنل در سراسر کشور زیر نظر اپراتور وجود دارد؛ چه بعنوان متخصص فنی، چه در دفاتر پشتیبانی امور مشترکین آن اپراتور و چه در بسیاری موارد دیگر که باید همکاری‌هایی درون سازمان صورا پذیرد تا نهایتا ارتباط برای کاربران آن اپراتور در سراسر کشور مقدور و میسر شود. زمانی که از شهر الف به شهر ب تماسی از طریق خطوط موبایلی برقرار می‌شود، با فرض اینکه هر دو کاربر، از یک اپراتور استفاده می‌کنند، به محض اینکه شماره فرد مقصد گرفته می‌شود، نزدیک‌ترین آنتن به کاربر، پیام‌ها و سیگنال‌ها را دریافت می‌کند، به سرورها ارجاع داده می‌دهد و سرورها آن سیگنال را پردازش نموده و محل کاربر مقصد را را می‌یابند.

حال اگر کاربر مقصد در موقعیت آنتن‌دهی باشد، ارتباط برقرار می‌شود. پس از اتصال تماس، این ارتباط پایدار می‌ماند تا زمانی که یکی از دو کاربر، آن را را قطع کند. یعنی بحث پوشش سخت‌افزاری و زیرساخت‌های ارتباطات سایبری، رکن اصلی ایجاد ارتباط در فضای سایبر است و بدون آن به هیچ عنوان برقراری ارتباط مقدور نیست.

با وجود تمامی هزینه‌های صورت گرفته، گسترش امکانات فنی و افزایش تعداد پرسنل اپراتورهای تلفن همراه در ایران، اما همواره مشترکانی هستند که از کیفیت نامطلوب برقراری ارتباط اپراتورها گله‌مند هستند.

*** پشت‌پرده سازمان اطلاعاتی – نظامی «وایبر»**

اکنون به نسبت توضیحات فنی ارائه شده، بیش از پیش توان فنی سازمان وایبر قابل درک است. کاربران وایبر می‌دانند که با این نرم‌افزار علاوه بر اینکه می‌توان تماس صوتی و متنی برقرار کرد، می‌توان فیلم، عکس و صوت هم ارسال نمود؛ یعنی در وایبر قابلیت‌هایی وجود دارد که هنوز ما در سیستم‌های موبایلی کشور شاهد آنها نبوده و بعضا اپراتورهای جدید قصد دارند این قبیل امکانات را به سرویس‌های خود اضافه نمایند.

شایان ذکر است در موارد مشابه نیز کیفیت وایبر بیش از اپراتورهای داخلی است. از سوی دیگر روشن است که وایبر یک شبکه جهانی است؛ یعنی از طریق آن می‌توان هر دو نقطه دلخواه در جهان را به هم مرتبط نمود. نکته سوم که مهم‌ترین نکته محسوب می‌شود رایگان بودن کلیه خدمات ارائه شده از سوی سازمان وایبر است.

پیش از این نرم‌افزارهایی مثل وی‌چت در کنار اینکه امکانات رایگان عرضه می‌نمودند؛ اما از تبلیغات هم استفاده می‌کردند که توسط آن سازمان متولی با دریافت هزینه تبلیغات از شرکت‌های سفارش‌دهنده، بخشی از هزینه‌ها را جبران می‌کرد اما در وایبر حتی این تبلیغات هم وجود ندارد. نرم افزار وایبر تمامی خدماتش را به‌صورت رایگان ارائه می‌دهد.

برای فهم ارتباطات نظامی پشت‌پرده وایبر تنها کافی است این پرسش بیان شود که «در مقایسه با اپراتورهای تلفن همراه داخلی که برای برقراری پوشش شبکه در سطح ملی، بودجه‌های بسیار سنگین و سرمایه بسیار بالایی را هزینه می‌کنند، چرا سازمان وایبر که در سطح جهانی هزینه‌های سنگینی متحمل می‌شود، هیچ هزینه‌ای بابت ارائه خدمات از کاربرانش نمی‌خواهد؟»

نکته حائز اهمیت این است که برای ایجاد و حفظ چنین کیفیتی جهت پوشش شبکه‌های وایبر در سطح جهان قطعا از بهترین، با کیفیت‌ترین و پیشرفته‌ترین سخت‌افزارها باید استفاده کند. علاوه بر این، اپراتورهای انسانی که آن‌ها را کنترل می‌کنند و مسئول پایش سیستم‌ها هستند، هزینه‌های خود را دارند. این هزینه‌ها از چه راهی تامین می‌شود؟ و سوالی که باید به آن پاسخ داده شود این است که چرا شرکتی مانند وایبر که تمام خدماتش در زمینه برقراری ارتباط است و برای تحقق این امر هزینه سنگینی را متحمل می‌شود، خدماتش را رایگان در اختیار همه قرار می‌دهد؟!

*** بودجه وایبر از کجا تامین می‌شود؟**

با توجه به پرسش فوق می‌توان دریافت که پشت‌پرده وایبر و دیگر شبکه‌های پیام‌رسان فوری، مقاصد اقتصادی وجود ندارد.

شرکت وایبر یک سازمان اطلاعاتی – نظامی اسرائیلی است و فرمانده آن تلمن مارکو[۴]، عضو سابق ارتش اسرائیل است. بودجه وایبر از سوی سازمان نظامی «یگان ملی اینتلیجنس سیگنال اسرائیل» (ISNU[۵]) تامین می‌شود که به صورت اختصاری به «یگان ۸۲۰۰»[۶] معروف است و تمامی اطلاعاتی که توسط وایبر از کاربرانش در سطح جهان به خصوص دشمنان اصلی اسرائیل یعنی ایران دریافت می‌کنند، در سرورهای اطلاعاتی این شرکت ذخیره می شود. برای هر کاربر پرونده ویژه‌ای تشکیل داده می‌شود که منحصر به‌فرد است. یکی از شیوه‌های شناسایی، شماره انحصاری سیم‌کارت هر کاربر است که از طریق آن می‌تواند در وایبر ثبت‌نام کند و موارد دیگری وجود دارد که در حوزه فنی بررسی می‌شود و از حوصله این بحث خارج است.

(http://fa.nsainfo.ir/wp-content/uploads/Talmon-Marco.png)

(http://fa.nsainfo.ir/wp-content/uploads/Unit-۸۲۰۰-۲۱.png)

یگان ملی اینتلیجنس سیگنال اسرائیل

در این سازمان شیوه‌های متعددی جهت شناسایی اشخاص وجود دارد و مشخص است که در هر لحظه، کدام کاربر در حال ارتباط است بدون آنکه با کاربر دیگری به اشتباه گرفته شود. اطلاعات کلی کاربرها دسته‌بندی و مورد استفاده قرار می‌گیرد. حداقل بهره‌ای که وایبر از اطلاعات کاربران می‌برد این است که آنها را به سازمان‌های اطلاعاتی دیگر در اسرائیل و خارج از اسرائیل خصوصا اروپای غربی و آمریکا می‌فروشد و در مقابل هزینه‌هایی بسیار بالاتر نسبت به سودی که می‌شد در ازای خدمات ارتباط از کاربران گرفت، دریافت می‌کند.

وایبر در سطوح بالاتر، موظف به شناسایی افرادی است تا برای اجرای پروژه‌های امنیتی، اطلاعاتی و نظامی دولت اسرائیل مورد استفاده قرار گیرند. از آنجا که اصلی‌ترین کشور هدف برای عملیات‌های تروریستی اسرائیل، جمهوری‌اسلامی ایران است، لذا توجه بسیار زیادی به کلیه ایرانیان عضو وایبر دارند تا توسط آنان اهداف مشخصی را دنبال نمایند.

به این ترتیب از قبل افراد را توسط وایبر شناسایی کرده و می‌دانند هر کاربر دارای چه روحیات، سلیقه‌ها، خصوصیات، گرایش‌های سیاسی و دینی، سطح و قدرت برقراری ارتباط اجتماعی و شغلی است یا حتی اطلاعاتی خصوصی‌تر مثل اینکه آیا تحصیلات عالی دارد، دایره ارتباطی‌اش با افراد گسترده است یا محدود، در شبکه اجتماعی برای مقاصد خاص آمده یا صرفا جهت سرگرمی عضویت یافته، محتاط است یا بی‌پروا و در نهایت اینکه آیا این شخص با وجود تمامی ویژگی‌هایی که با آن شناخته شده و در پرونده‌اش در سازمان اسرائیلی وایبر ثبت شده است، برای پروژه‌ها و مقاصد خاص آن‌ها مناسب است یا خیر؟ می‌توان او را تطمیع کرد یا باید از طریق تهدید به انجام کاری وادارش کرد؟

از این جهت، سنگین‌ترین تهدیدات در حوزه امنیت ملی، در حال حاضر از طریق فضای سایبر در بخش نرم‌افزارهای پیام‌رسان فوری حادث می‌شود که شاخص‌ترین آن ها وایبر است. البته این موارد درباره دیگر نرم‌افزارهای پیام‌رسان فوری موبایلی هم صادق است. به عنوان مثال در نرم افزار تانگو پیش از این امکانی وجود داشت که شخص می‌توانست فارغ از اینکه خودش در کجای جهان قرار دارد در کشور هدف، شهری خاص و سپس خیابان خاصی را انتخاب کند و در آن خیابان به شعاع سه کیلومتر درخواست نماید تا هر کاربر تانگو را شناسایی نماید و برای برقراری ارتباط، به شخصی که در حال جست‌وجو است معرفی بشود.

شاید به ظاهر این یک امکان فوق‌العاده است و بسیاری از افراد را به تانگو جذب کرد؛ اما تنها یک لحظه باید در نظر داشت که مهیا ساختن چنین امکانی از حیث ابزارهای فنی و مهم‌تر از آن مجوزهای دسترسی در کشورهای مختلف، چه سطوح بالایی از امنیت را نیاز دارد؟ این امکان فقط از طریق استفاده از ماهواره‌های نظامی امکان‌پذیر است که البته اخیرا این امکان برداشته شده است. اما به واسطه اینکه چنین امکانی فقط با ماهواره‌های نظامی میسر است به راحتی اثبات می‌کند که ابزار تانگو هم یک نرم‌افزار نظامی می‌باشد.

این موارد درباره تمام نرم‌افزارهای پیام‌رسان فوری که تا الان شناخته شده است، وجود دارد. ۵۰ الی۶۰ نرم‌افزار اصلی که در ایران وجود دارد، از مشاهیری نظیر اینستاگرام، وایبر، وی‌چت تا مواردی مانند تلگرام و هایک که کمتر معروف هستند.

*** کلام آخر**

کاربران این حق را دارند پیش از استفاده از این نرم‌افزارها، از خطرات امنیتی آن در حوزه فردی، حریم خانوادگی و حتی سطح امنیت ملی که با استفاده از این نرم‌افزارها برایشان ایجاد می‌شود، آگاهی پیدا کنند و قطعا کمتر کسی است که از این موارد آگاهی یابد و باز هم این خطرات را نادیده بگیرد و به روال پیشین خودش ادامه بدهد، بی‌پروا و بی‌محابا تمامی اطلاعاتش را از طریق این سیستم‌ها رد و بدل کند و خودش را در معرض افشا و شناخته شدن قرار بدهد.