هوالخیر

فلسفه‌ی امنیتی – اطلاعاتی سرویس‌های پیام‌رسان فوری

محمدعلی شکوهیان‌راد

اردیبهشت ۱۳۹۴

بیان مطلب

بشر امروزی با گذر از اعصار پیشین نظیر عصر سنگ، عصر کشاورزی و عصر صنعت، به دوره‌ی جدیدی ورود یافته که «عصر اطلاعات» نامیده می‌شود.

هر کدام از اعصار یاد شده به دلیل دارا بودن ویژگی‌های خاص و منحصر به‌فرد، تبعاً شرایط خاصی را نیز موجب شده است. از جمله‌ی این شرایط، مسأله چگونگی دست‌یابی به قدرت برای تحمیل نظر خود بر دیگران بود. حوزه قدرت و برتری‌جویی در هر عصر، کاملاً گزاره‌مند و البته متفاوت از دیگر اعصار است. در واقع در هر عصر، عاملی که منشأ حیات و بقای مردم و ملت‌ها است، در صورتی که بتوان به‌صورت انحصاری آن را در اختیار گرفت، منشأ قدرت و برتری است.

ردیف	دوره	عامل قدرت	چگونگی اکتساب
۱	عصر سنگ	--	--
۲	عصر کشاورزی	مَلاکی و زمین‌داری	جنگ و نزاع با دیگر مَلاکان
۳	عصر صنعت	تکنولوژی منحصر به‌فرد	ایده‌پردازی و طراحی
۴	عصر اطلاعات	اشراف اطلاعاتی	سیستم‌های جمع‌آوری اطلاعات

عامل قدرت در عصر اطلاعات «اشراف اطلاعاتی» است و میزان قدرت به‌طور مستقیم با میزان اشراف اطلاعاتی در ارتباط است. از این رو در اختیار گرفتن عوامل کسب اطلاعات موجب در اختیار گرفتن قدرت است. از آنجا که ماهیت اطلاعات بی‌جهت است و جهت‌مندی و کاربرد آن به بینش و اهداف تحلیل‌گر باز می‌گردد، اطلاعات در تمامی عرصه‌های زندگی بشری از سطح فردی تا اجتماعی نقشی حیاتی ایفا می‌کند.

به مرور زمان با آغاز انتقال سیستم‌های حاکم بر کشورها از «ارگانیک»[1] به «سایبرنتیک»[2]، شیوه جمع‌آوری اطلاعات نیز دستخوش تغییرات بنیادین شد. در مدل حاکمیت از نوع ارگانیک پنج مؤلفه سیاست، اقتصاد، جامعه، فرهنگ و امنیت مبنای طرح‌ریزی قدرت است و هدف، حفظ حاکمیت از راه ارتقای هر مؤلفه پایه‌ای در این مدل است. همچنین سبک کسب اطلاعات از طریق ارسال عوامل نفوذی به منابع اطلاعات و راهبردهای حکومتی هر کدام از مؤلفه‌های یاد شده است.

اما در مدل سایبرنتیک با دو مؤلفه‌ی اطلاعات و انرژی، شرایط به‌گونه‌ای متحول می‌شود که دیگر حتی عناصر مدل ارگانیک، اثر و نقش سابق خود را از دست می‌دهند. در این مدل هدف، حفظ حاکمیت از طریق پایش و کنترل مستمر انواع تهدیدات است و از آنجا که منشأ تهدیدات برانداز، انسان است، لذا انسان‌ها در سطوح مختلف از فردی تا ملی باید تحت نظارت مداوم باشند.

---

[1] Organic
[2] Cybernetic

در ادبیات سیستم سایبرنتیک، سه واژه اساسی مطرح است که باید به‌خوبی فهم شود:

ردیف	واژه	مفهوم
۱	Monitoring	اشراف اطلاعاتی همراه با ذخیره‌ی اطلاعات به‌صورت خام، بدون آگاهی نظارت‌شونده
۲	Surveillance	اشراف اطلاعاتی دقیق و هدفمند که منجر به تولید اطلاعات راهبردی شود، غالباً بدون آگاهی نظارت‌شونده
۳	Control	اشراف اطلاعاتی به همراه اقدام عملیاتی در راستای تغییر وضعیت تحت اشراف در جهت خواسته‌های اشراف‌گر، قالباً با آگاهی نظارت‌شونده

آنچه که در مجموع نظارت این سیستم صورت می‌پذیرد از سطح مانیتورینگ بر جوامع آغاز شده و در نهایت به کنترل همان جوامع ختم می‌شود و این چرخه به‌صورت ممتد ادامه دارد.

اما تفاوت اساسی تهدیدات امنیت ملی علیه یک کشور زمانی که در براندازی‌اش از مدل تهدیدات ارگانیک استفاده می‌شود تا زمانی که مدل سایبرنتیک به ایجاد تهدید برای آن می‌پردازد در اینست که تهدیدات ارگانیکی، سطح کلان یک جامعه یعنی حاکمیت را هدف می‌گیرند. به‌عنوان مثال با حصر اقتصادی علیه یک کشور سعی می‌کنند گردش مالی و تأمین اقتصادی آن حکومت را تضعیف کنند یا با تهاجم فرهنگی، مقاصد فرهنگی که حکومت برای جامعه‌اش در نظر دارد منحرف و بی‌اثر سازند. لذا جهت تهدیدات از بالا به پایین است. اما در مدل سایبرنتیک این موضوع عمدتاً به‌صورت عکس عمل می‌کند. بدین طریق که بر تمامی جامعه نظارت اطلاعاتی از سوی دشمن انجام می‌گیرد و خطاهای هر شخص چه در بُعد فردی و چه در بُعد اجتماعی ثبت می‌گردد تا نهایتاً در موقع مورد نیاز، از طریق فشار شخصی به او، به تبع یک کشور تحت فشار و تهدید قرار گیرد. بدین ترتیب جهت تهدیدات در مدل سایبرنتیک از پایین به بالا است.

به‌عنوان نمونه، پیش از شروع جنگ ۸ روزه رژیم صهیونیستی علیه نوار غزه، «زیبی لیونی»[۳] وزیر سابق امور خارجه‌ی رژیم صهیونیستی اعلام کرد «با دو نفر از سران کشورهای عربی رابطه‌ی نامشروع جنسی داشته و در همان حین از آنها اطلاعات لازم را به‌دست آورده است»[۴] و بدین گونه با گروگان‌گیری اطلاعاتی از یک شخص، به‌تبع یک کشور را با تهدید ملی روبرو ساخت.

اما سؤال بسیار مهم در اجرای مدل سایبرنتیک این است که مانیتورینگ و نظارت[۵] بر تمامی جوامع جهان چگونه میسر است؟! چگونه می‌شود از قریب به ۸ میلیارد نفر جمعیت جهان جمع‌آوری اطلاعات نمود و اینکه آیا اساساً چنین عملی مقدور است؟

---

[3] Tzipi Livni

[۴] خبرگزاری تیرپرس. عنوان خبر: «وزیر خارجه پیشین اسرائیل: با مقامات عربی رابطه جنسی داشتم و فیلمش نیز موجود است»

[5] Surveillance

ارائه‌ی پاسخ جامع و کامل به این سؤال نیازمند بررسی و بازخوانی تاریخ راهبردی تکنولوژی نظامی سایبری از سال ۱۸۴۰ میلادی تا سال ۲۰۱۵ است. یعنی از زمان گسترش تلگراف تا عصر تکنولوژی‌های پیچیده امروزی. از این رو از حوصله این متن خارج است اما با بررسی آخرین نسل تکنولوژی سایبری یعنی «پیام‌رسان‌های فوری»[6] می‌توان به‌خوبی دریافت که پاسخ به پرسش فوق چگونه امکان یافته است.

جزء اصلی راهبرد سایبرنتیک، توان زیرساخت فنی آن است. برای نظارت اطلاعاتی بر تمام ملل و به تبع، کنترل آنها، باید ابزاری داشت که اولاً توانایی جمع‌آوری هر نوع اطلاعات اعم از صوتی، تصویری، متنی، مکانی و ... را داشته باشد، ثانیاً در کسب اطلاعات حاصله از سوی سازمان کنترل‌گر نیازمند یک نیروی انسانی نباشد وگرنه برای هر دستگاه کنترل‌کننده یک اپراتور لازم است که عملاً غیر ممکن است، ثالثاً باید افراد مصرف‌کننده به آن اعتماد کامل داشته باشند و براحتی اطلاعات‌شان را به سیستم مذکور بسپارند و نهایتاً اینکه باید جز ضروریات زندگی بشر باشد در غیر اینصورت از روند اطلاعاتی زندگی خارج می‌گردد.

با چنین مفروضاتی، روند تکنولوژی به ایجاد پیام‌رسان‌های فوری رسید. یک برنامه پیام‌رسان فوری، فارغ از سازمان تولیدکننده‌اش به‌صورت ذاتی توانایی جمع‌آوری کلیه اطلاعات شخصی و محرمانه فرد و محیط اطرافش را در قالب صوت، متن، تصویر، موقعیت مکانی، اطلاعات بیومتریک شخص نظیر سرعت تایپ، اسکن قرنیه چشم، تونالیته صدای وی، برنامه‌های مورد استفاده کاربر که بر روی پلت‌فرم موبایلی یا سیستمی او نصب شده و ... را دارد.

این اطلاعات به‌صورت خام از مبدأ یعنی موبایل کاربر به سرورهای ذخیره اطلاعات در سازمان متولی نرم‌افزار ارسال شده، در پرونده شخصی کاربر قرار می‌گیرد. سپس توسط نرم‌افزارهای هوش مصنوعی روانشناسی و یک اپراتور انسانی که متخصص تحلیل اطلاعات است، کلیه سلایق، افراد مرتبط، خلق و خوی شخصی، گرایشات سیاسی، مذهبی، درجه روابط عمومی، قدرت تکلّم، درجه سایبورگ و ... او بدست می‌آید.

بدین ترتیب کلیه کاربران سرویس‌های پیام‌رسان فوری چنین پرونده اطلاعاتی قوی و کاملی در سازمان‌های متولی نرم‌افزارهای مورد استفاده‌شان دارند که اگر به‌صورت مکتوب به خودشان داده شود هرگز باور نمی‌کنند تا این حد دقیق و بی‌نقش مورد تحلیل مداوم بوده‌اند. مواردی که بعضاً حتی خود شخص بر آنها آگاهی خود آگاه ندارد!

اما سؤال مهم دیگر اینست که اگر شرکت‌های ارائه‌دهنده این امکانات نظیر وی‌چت[7] خصوصی بوده و با حاکمیت کشورهای کنترل‌گر ارتباط ندارند، پس چگونه چنین مسئله‌ای ممکن است؟! به‌عبارت دیگر چگونه کنترل دولتی از طریق شرکت‌های خصوصی صورت می‌پذیرد؟

---

[6] Instant Messaging
[7] We Chat

شاید اگر تا پیش از سال ۲۰۱۳ این مسائل مطرح می‌شد، با پاسخی مثل «داشتن توهم توطئه» از سوی جامعه مواجه می‌شد اما اکنون که در حدود دو سال از افشاگری‌های «ادوارد اسنودن»[۸]، پیمانکار اطلاعاتی «آژانس امنیت ملی»[۹] می‌گذرد و هزاران صفحه سند رسمی و غیر رسمی مبنی بر همکاری‌های پشت‌پرده شرکت‌های خصوصی محبوب سایبری مثل گوگل، ماکروسافت، فیس‌بوک و ... را منتشر کرده است، دیگر فضای جامعه برای پذیرفتن این وقایع تلخ، موضع مخالف اتخاذ نمی‌کند.

هر شرکت در حوزه تکنولوژی سایبری، برای دریافت مجوز تجاری و انتشار محصولش، باید استانداردهای آژانس امنیت ملی آمریکا را رعایت کند در غیر اینصورت موفق به حیات اقتصادی نخواهد شد.

از سوی دیگر بر اساس بسیاری از اسناد منتشر شده، جمهوری‌اسلامی ایران، هدف اصلی و اول تمامی سازمان‌های اطلاعات سایبری غرب به‌ویژه انگلیس و آمریکا است و این موضوع تا حدی عمیق است که برای از دست ندادن کوچکترین اطلاعات ملت ایران، بعضاً اشراف اطلاعاتی بر دیگر مناطق کم اهمیت‌تر جهان را پایین آورده و از توان فنی آن برای نظارت بیشتر بر کاربران ایرانی استفاده نموده‌اند.

در حال حاضر ۴۱ برنامه پیام‌رسان فوری در ایران بین کاربران رایج است که بظاهر همگی خصوصی است و میان ایرانیان محبوبیت زیادی دارد اما با نگاهی به پشتیبانان و مالکان اطلاعاتی، امنیتی و نظامی هر شرکت، واقعیت پشت‌پرده بگونه‌ای دیگر شفاف می‌گردد.

لیست مهم‌ترین و رایج‌ترین برنامه‌های پیام‌رسان فوری در ایران به همراه شرکت تولیدکننده آن و نهایتاً سازمان اطلاعاتی اصلی که اطلاعات کاربران نرم‌افزار را مورد استفاده قرار می‌دهد در جدول زیر آمده است:

ردیف	نام نرم‌افزار	لوگو	سازمان اولیه	سازمان نهایی
۱	Aim		AOL	آژانس امنیت ملی آمریکا (NSA)
۲	Beetalk		Garena	مدیریت سیگنال‌های استرالیا (ASD)
۳	Bisphone		Bistalk Telecom AG	سرفرماندهی ارتباطات دولتی انگلیس (GCHQ) سازمان اطلاعات آلمان (BND)
۴	BlackBerry		بلک‌بری کانادا	سازمان امنیت ارتباطات کانادا (CSE)
۵	Chat on		سامسونگ	مدیریت سیگنال‌های استرالیا (ASD)
۶	Cubie			آژانس امنیت ملی آمریکا (NSA)
۷	Facebook		فیس‌بوک	آژانس امنیت ملی آمریکا (NSA) آژانس اطلاعات مرکزی آمریکا (CIA)
۸	Facetime		اَپل	آژانس امنیت ملی آمریکا (NSA)

[8] Edward Snowden
[9] NSA: National Security Agency

۹	Frankly		فرانکلی	مدیریت سیگنال‌های استرالیا (ASD)
۱۰	Frontback			آژانس امنیت ملی آمریکا (NSA)
۱۱	Glide		Glide Talk	آژانس امنیت ملی آمریکا (NSA)
۱۲	Google Talk		گوگل	آژانس امنیت ملی آمریکا (NSA)
۱۳	Group Me		ماکروسافت	آژانس امنیت ملی آمریکا (NSA)
۱۴	Hangouts		گوگل	آژانس امنیت ملی آمریکا (NSA)
۱۵	Hike		سافت بانک (ژاپن و هند)	سرفرماندهی ارتباطات دولتی انگلیس (GCHQ) آژانس امنیت ملی آمریکا (NSA)
۱۶	ICQ		Mirabilis (اسرائیل)	یگان ملی اینتلیجنس سیگنال اسرائیل (ISNU)
۱۷	Instagram		فیس‌بوک	آژانس امنیت ملی آمریکا (NSA)
۱۸	IRC		Jarkko Oikarinen	سازمان‌های اطلاعاتی متفقین
۱۹	Kakao Talk		گروه کاکائو (کره جنوبی)	مدیریت سیگنال‌های استرالیا (ASD)
۲۰	Kik		دانشگاه واترلو کانادا	سازمان امنیت ارتباطات کانادا (CSE)
۲۱	Libon		Orange S.A فرانسه	آژانس اینتلیجنس فرانسه (DGSE)
۲۲	Line		شرکت لاین ژاپن	مدیریت سیگنال‌های استرالیا (ASD)
۲۳	Maaii		هنگ‌کنگ	مدیریت سیگنال‌های استرالیا (ASD)
۲۴	Nimbuzz		Nimbuzz V.B	سازمان جمع‌آوری سیگنال‌های ملی هلند (NSCO)
۲۵	OoVoo		ooVoo LLC (آمریکا)	آژانس امنیت ملی آمریکا (NSA)
۲۶	Palringo		Martin Rosinski انگلیس	سرفرماندهی ارتباطات دولتی انگلیس (GCHQ)
۲۷	Path		Path (آمریکا)	آژانس امنیت ملی آمریکا (NSA) مدیریت سیگنال‌های استرالیا (ASD)
۲۸	QQ		Tencent چین	آژانس امنیت ملی آمریکا (NSA) مدیریت سیگنال‌های استرالیا (ASD)
۲۹	Rounds			آژانس امنیت ملی آمریکا (NSA)
۳۰	Skout		Skout	آژانس امنیت ملی آمریکا (NSA)
۳۱	Skype		ماکروسافت	آژانس امنیت ملی آمریکا (NSA)
۳۲	Snap Chat		براون و اشپیگل آمریکا	آژانس امنیت ملی آمریکا (NSA)

۳۳	Tango		Uri Raz & Eric Setton آمریکا	آژانس امنیت ملی آمریکا (NSA)
۳۴	Tapatalk		Tapatalk, Inc.	آژانس امنیت ملی آمریکا (NSA)
۳۵	Telegram		Telegram Messenger LLP آلمان	سازمان اطلاعات آلمان (BND) آژانس امنیت ملی آمریکا (NSA)
۳۶	Text Secure		Stuart Anderson آمریکا	آژانس امنیت ملی آمریکا (NSA)
۳۷	Tic Toc		کره جنوبی	مدیریت سیگنال‌های استرالیا (ASD)
۳۸	Tinder		Tinder آمریکا	آژانس امنیت ملی آمریکا (NSA)
۳۹	Twitter		Odeo آمریکا	آژانس امنیت ملی آمریکا (NSA)
۴۰	Upp Talk		Yuilop آمریکا	آژانس امنیت ملی آمریکا (NSA)
۴۱	Viber		یگان ملی اینتلیجنس سیگنال اسرائیل (ISNU)	آژانس اطلاعات ارتش اسرائیل - (AMAN)
۴۲	Vine		Twitter	آژانس امنیت ملی آمریکا (NSA)
۴۳	WeChat		Tencent چین	آژانس امنیت ملی آمریکا (NSA) مدیریت سیگنال‌های استرالیا (ASD)
۴۴	What's app		یاهو (به‌طور غیر مستقیم)	آژانس امنیت ملی آمریکا (NSA)
۴۵	Yahoo!		یاهو	آژانس امنیت ملی آمریکا (NSA)

نتیجه‌گیری

کافی است یک بار با خود بیندیشیم اگر یک شرکت فعال در حوزه تکنولوژی سایبر همانند وایبر، تمامی درآمد و چرخه اقتصادی‌اش که منتج به سودآوری می‌شود از طریق خدماتی است که ارائه می‌دهد و از سوی دیگر برای ایجاد زیرساخت فنی تأمین خدماتش آن‌هم در سطح جهان، هزینه‌های بسیار سنگین بالغ بر چند ده میلیارد دلار را متحمل گردیده و همچنین با هزینه‌های سنگین دیگری از قبیل حقوق پرسنل، تعمیر و نگهداری سیستم‌ها، هزینه دیتا، پرداخت مالیات و ... به‌صورت مستمر مواجه است، چرا ثمره تمامی هزینه‌های صرف شده که شامل امکانات ارتباطی متنی، صوتی و تصویری است را به رایگان در اختیار تمامی کاربران قرار می‌دهد؟!

کافی است برای فهم بهتر این تناقض، نسبت هزینه‌های صرف شده در تجهیز زیر ساخت یک اپراتور تلفن همراهی داخلی در مقایسه با قیمت ارائه خدمات‌اش به کاربران را بسنجیم و ضمناً مد نظر داشته باشیم

اپراتورهای تلفن همراه در ایران در حوزه ملی ارائه خدمات می‌کنند نه بین‌المللی؛ حال آنکه نرم‌افزارهای فوق در سطح جهان، هم خدمات بیشتری ارائه می‌کنند و هم از کیفیت بالاتری برخوردارند.

کافی است یکبار از خود بپرسیم چرا ج. ا. ایران در هر زمینه‌ای حتی تأمین چرخ هواپیمای مسافربری با حصر اقتصادی و تحریم مواجه است اما در سه حوزه:

۱- سخت‌افزارهای سایبری اعم از لب‌تاب، تبلت، گوشی همراه و ...

۲- نرم‌افزارهای سایبری نظیر انواع سیستم‌عامل رایانه و گوشی همراه، برنامه‌های کاربردی تخصصی، برنامه‌های کاربردی عمومی و ...

۳- پهنای باند و دیتا

نه تنها تحریم، بلکه حتی تهدید به تحریم نشده است؟!

این سخن گران‌بار امام خامنه‌ای(مدظله‌العالی) را فراموش نکنیم که فرمودند: «مراقب دشمن باشید؛ دشمن را خوب بشناسید؛ مبادا از شناسایی دشمن غفلت کنید... هیچ کس به‌خاطر غفلت ستایش نمی‌شود. هیچ‌کس به‌خاطر چشم‌ها را بر هم گذاشتن، مدح نمی‌شود. اگر بر آدم غافل ضربه‌ای وارد شد، اوّل کسی که مسئول و مذموم است، خود اوست؛ مراقب باشید.»[۱۰]

[۱۰] بیانات در دیدار با دانشجویان مورخ ۲۱/تیر/۱۳۷۸