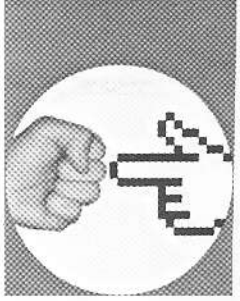


هیس... دارند گوش می‌کنند

روزنامه‌نگاری که برای نخستین بار «اشلون»(یکی از شبکه‌های بزرگ جاسوسی الکترونیکی) را کشف کرد، اکنون فاش می‌سازد که چگونه سیستم نظارت و مراقبت بین‌المللی به همه‌ی ما دسترسی دارد

«دانکن کمبل»
روزنامه‌نگار جستجوگر اسکاتلندی

در دورافتاده‌ترین نقاط سراسر جهان، از رشته‌کوه‌های «پامیر» در چین گرفته تا سواحل باتلاقی شمال استرالیا و تا نوک توده‌های مرجانی جزایر اقیانوس هند، می‌توان شاهد مناطقی پر از توپ‌های عظیم گلف بود. این گوی‌های سفیدرنگ صاف و متقارن که در فاصله‌ی ۳۰ تا۵۰ متری یکدیگر قرار دارند، در میان شالیزارهای شمال ژاپن و تاکستان‌ها و کوهستان‌های جزیره‌ی جنوبی نیوزیلند هم به چشم می‌خورند.

این گوی‌های دسته‌دسته، آشکارترین نشانه‌های شبکه‌های الکترونیکی پنهانی هستند که جهان را زیر نظر دارند. هر گوی پر از بشقابک‌های ردگیر ماهواره‌ای است که میلیون‌ها نمابر، نامه الکترونیکی، تماس تلفنی و اطلاعات کامپیوتری را(که سیر تمام امور سیاسی و تجاری از طریق آنهاست) بی‌سروصدا به درون خود می‌کشد و بررسی می‌کند. پیام‌های تماس‌گیرندگان بدون آن که خود بدانند، از درون این گوی‌ها به شبکه‌های کامپیوتری می‌رود و از آنجا به گوش کسانی می‌رسد که شاید آن سوی کره‌ی زمین نشسته‌اند.

همزمان با روند جهانی‌شدن، و در حالی که مخابرات و ارتباطات بین‌المللی نقش محوری در امور انسان یافته، این شبکه‌های شنود به‌طرز چشمگیری گسترش یافته‌اند. این شبکه‌ها بخشی از سیستم‌هایی هستند که «جاسوسی علائم» یا «سیگینت» نامیده می‌شوند و توسط تعداد انگشت شماری از کشورهای پیشرفته اداره می‌گردند.

سالیان سال، شبکه‌های «سیگینت»، مخفی بودند: بحث پیرامون وجود چنین شبکه‌های به شدت سرکوب می‌شد یا حتی در برخی کشورها اصلاً طبق قانون چنین بحث‌هایی ممنوع بود. اکنون پارلمان اروپا به‌طور جدی در حال بررسی سازمان‌های «سیگینت» و تأثیر آنها بر حقوق بشر و تجارت بین‌المللی است. کانون توجه اروپا روی شبکه «اشلون» متمرکز است. این شبکه به یک رشته پایگاه‌های شنود در حدود ده کشور متکی است که در این پایگاه‌ها همه‌ی ارتباطات و مخابرات ماهواره‌ای بین‌المللی شنود و پردازش می‌شود. «اشلون» فقط بخشی از یک شبکه عظیم است که توسط ایالات‌متحده و متحدان انگلیسی‌زبان آن(بریتانیا، کانادا، استرالیا و نیوزیلند) اداره می‌شود و به اتحادUKUSA موسوم است؛ این نام برگرفته از توافقی پنهانی در سال۱۹۴۸ است که موجب پیدایش این اتحاد شد. کمتر علامت و پیامی از دید شبکه‌یUKUSA پنهان می‌ماند. این شبکه پیامهایی را که از روی اینترنت، کابل‌های زیردریایی و امواج رادیویی انتقال می‌یابد و همچنین پیام‌های ارسالی از تجهیزات مستقر در سفارت‌خانه‌ها را شنود می‌کند. این شبکه حتی به کمک ناوگانی از ماهواره‌ها در فضا نیز فعال است.

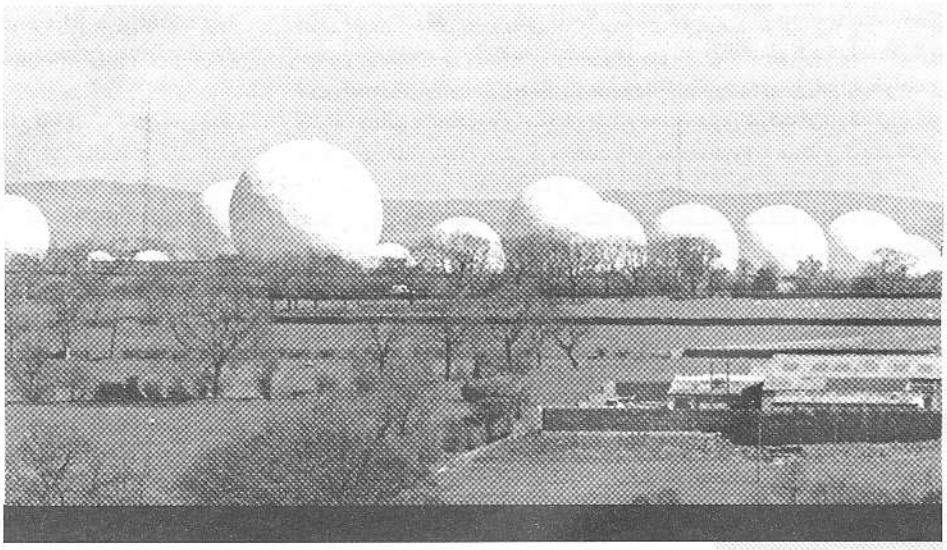
تاریخچه‌ی سیستم‌هایی شبیه «اشلون» به قدمت خود رادیو است. نخستین رسوایی بین‌المللی بر سر شنود پنهانی در دهه‌ی۱۹۲۰ رخ داد؛ همان زمان که مجلس سنای ایالات متحده دریافت که جاسوسان بریتانیایی از هر پیامی که توسط شرکت‌های تلگراف آمریکایی ارسال می‌شود رونوشت تهیه می‌کنند. شبکه‌های بین‌المللی امروزی در اوائل دوران جنگ سرد پایه‌گذاری شدند؛ همان زمان که بسیاری از کشورهای غربی به‌طور مشترک شروع کردند به نظارت و مراقبت فعالیت‌های اتحاد شوروی سابق.

از واژه‌ی «بمب» نترسید

چه کسی به پیام‌ها گوش می‌کند و چرا؟ دولت‌ها به‌طور رسمی فقط به این اذعان می‌کنند که سیستم‌های نظارت و مراقبت معطوف به خطرات مورد توافق همگانی است؛ خطراتی همچون گسترش تسلیحات، تروریسم، قاچاق مواد مخدر و تبهکاری‌های سازمان‌یافته. اما این فقط نوک کوه یخ است. هدف اصلی جاسوسی، پیام‌های دیپلماتیک‌و نقشه‌های نظامی دیگر دولت‌ها و همچنین جمع‌آوری اطلاعات تجاری است. در واقع، در سال۱۹۹۲، ایالات متحده اولویت‌های‌جاسوسی خود را تغییر داد و به گفته‌ی «رابرت گیتس»، رییس وقت سازمان سیا،۴۰ درصد فعالیت‌های جاسوسی را اقتصادی یا «ماهیتاً اقتصادی» تشخیص داد. سازمان‌های بین‌المللی و غیردولتی نظیر سازمان «عفو بین‌الملل» و گروه «صلح‌سبز» نیز جز هدف‌های جاسوسی هستند.

درست است کهUKUSA بزرگترین شبکه جهان است اما فرانسه، آلمان و فدراسیون روسیه نیز سیستم‌های مشابه خاص خود را دارند. کشورهای اسکاندیناوی و خاورمیانه، از جمله فلسطین اشغالی، عربستان سعودی و کشورهای حوزه‌ی خلیج(فارس) نیز هرچند در مقیاسی بسیار کوچک، دارای این گونه سیستم‌ها هستند. بر اساس محاسبات من از گزارش‌های منتشر شده‌ی‌سال پیش پارلمان اروپا، بودجه‌ی کل سازمان‌های «سیگینت» دولتی بالغ بر۲۰ میلیارددلار در سال می‌شود.

با وجود ابعاد خیره‌کننده‌ی شبکه‌ی «اشلون» و



شبکه‌های خواهر آن، مطبوعات به اشتباه گزارش کرده‌اند که این شبکه می‌تواند «همه‌ی نامه‌های الکترونیکی، تماس‌های تلفنی، و ارتباطات دورنگار» را شنود کند. اما این شبکه به‌هیچوجه نمی‌تواند محتوای همه‌ی تماس‌های تلفنی را شناسایی کند. این یک خیال محض است که اگر کسی در نامه‌ی الکترونیکی خود واژه‌ی «بمب» را تایپ کند، باعث روشن شدن یک دستگاه ضبط در یک پایگاه نامعلوم می‌شود. از هر یک میلیون پیام و تماس تلفنی که شنود می‌شود، شاید کمتر از ۱۰ پیام برای اهداف جاسوسی استفاده داشته باشد. از ارتباطات کاملاً شخصی صرف‌نظر می‌شود مگر این که شخص موردنظر، آدم «مهمی» باشد؛ مثلاً یک سیاستمدار یا رئیس یک شرکت بزرگ و یا خانواده‌های آنها.

با این حال، شبکه‌ی UKUSA قدرت این را دارد که به اکثر ارتباطات ماهواره‌ای جهان دسترسی پیدا کند و پیام‌های آن را پردازش کند و به کشورهای مورد نظر خود ارسال دارد. این سیستم، برتری سیاسی ناعادلانه و عظیمی به کشورهای مشارکت کننده در این شبکه می‌دهد، زیرا اکثر کشورهای در حال توسعه استطاعت آن را ندارند که تخصص‌ها و تجهیزات لازم برای حفظ حریم‌شخصی و امنیت شبکه‌های خودشان را تأمین کنند.

جاسوسی دولت برای مردم

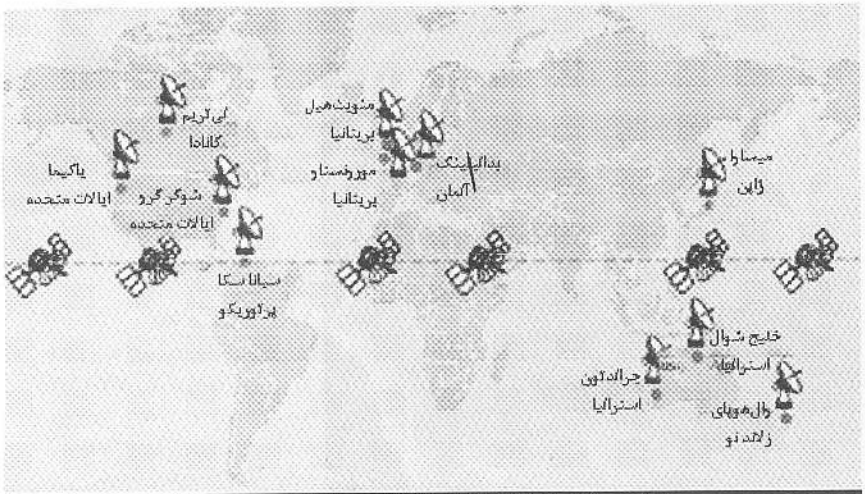
اخبار وجود چنین شبکه‌هایی در دهه‌ی ۱۹۷۰ به بیرون درز کرد. این همان زمانی بودکه سازمان‌های جاسوسی ایالات متحده بابت ماجرای «واترگیت» مورد تحقیق‌وتفحص قرار گرفته بودند. در آن ماجرا، «ریچارد نیکسون» رئیس‌جمهور سابق ایالات متحده برای رقبای انتخاباتی خود میکروفن‌های الکترونیکی کار گذاشته بود. از آن زمان تاکنون بسیاری کسان ابعاد و اثرات جاسوسی «سیگینت» را فاش ساخته‌اند و نسبت به آن هشدار داده‌اند.

من نخستین بار در دهه‌ی ۱۹۷۰، مطلبی درباره‌ی جاسوسی الکترونیکی توسط بریتانیا نوشتم. من که در آن زمان مشغول تحصیلات دانشگاهی در رشته فیزیک بودم، متوجه شدم که حومه‌ی شهر پر شده است از پایگاه‌های اسرارآمیز رادیویی و ماهواره‌ای. من در سال ۱۹۷۶، برپایه‌ی تحقیق‌وتفحص نمایندگان کنگره آمریکا که یک سال پیشتر فعالیت‌های «سازمان امنیت ملی آمریکا» را برملا کرده بودند، نقش بریتانیا را در فعالیت‌های این سازمان فاش ساختم. مقامات، از این که می‌دیدند گاو مقدس‌شان با آن راز ابدی و بی‌خدشه، سلاخی شده، مات و مبهوت مانده بودند. بلافاصله پس از انتشار مقاله‌ی من، همکار آمریکایی‌ام به اتهام این که وی «تهدیدی علیه امنیت ملی» است از بریتانیا اخراج شد.

سپس دولت، من و یک روزنامه‌نگار دیگر و منبع اطلاعاتی ما را دستگیر کرد. مقامات جرأت نکردند ما را به جاسوسی برای یک کشور بیگانه متهم کنند. «جرم» ما جاسوسی دولت برای مردم بود. اگر محاکمه شده بودیم، هیچ بعید نبود با حبس‌های سنگین روبه‌رو شویم.

در بیست‌سالی که از آن زمان می‌گذرد، با چرخش زاویه‌ی دید هیأت تحقیق‌وتفحص کنگره آمریکا به سوی سازمان‌های «سیگینت»، پنهانکاری دولت نیز تخفیف یافته است. در بریتانیا در دهه‌ی ۱۹۸۰، یک بحث پرجنجال بر سر ممنوعیت عضویت کارکنان «اداره مرکزی مخابرات دولت» در اتحادیه‌های صنفی، باعث شد که قضیه به ضرر این اداره تمام شود و همه توجه‌ها به فعالیت‌های جاسوسی این اداره جلب گردد.

اینترنت و رشد فرهنگ عمومی اطلاع‌رسانی باعث شده که این تحولات حتی پیشتر هم برود. اکنون، حتی «اداره مرکزی مخابرات دولت» و «سازمان امنیت ملی آمریکا» دارای پایگاه‌های اینترنتی هستند تا خاطر شهروندان UKUSA را آسوده بدارند که آنها هدف این سازمان نیستند. چنین تضمینی برای بقیه مردم دنیا وجود ندارد: شهروندان دیگر کشورها اصلاً حقی بابت مصون ماندن حریم‌شخصی خود ندارند. کشورهایی که ارتباطات آنها را شنود می‌کنند آزاد هستند که از امکانات



کمتر اطلاعاتی از تور گسترده‌ی «اشلون» بیرون می‌ماند

جاسوسی در هرجایی که میل داشته باشند،بهره بگیرند.

چنین رویه‌ای در واقع یک تخطی آشکار از بیانیه جهانی حقوق بشر و همچنین معاهده‌ی اروپایی حقوق‌بشر و معاهده‌ی بین‌المللی مخابرات است؛ معاهده‌ای که ضامن حفظ حریم‌شخصی در مخابرات بین‌المللی است. در واقع سازمان‌های «سیگینت» معاهداتی را که قدمتی دیرینه دارند، پایمال می‌کنند.

شاید تک‌تک افراد هرگز نفهمند که مورد جاسوسی قرار گرفته‌اند اما چه بسا سازمان‌ها و کشورهای آنها بهای سنگینی بابت این امر بپردازند. در جریان مذاکرات تجاری، سازمان‌های «سیگینت» می‌توانند پیام‌های یک کشور تولیدکننده را شنود کنند تا بفهمند حد طاقت آن کشور در چانه‌زنی کجاست. مذاکره‌کنندگان کشورهای توسعه‌یافته که مسلح به چنین گزارش‌های محرمانه‌ای هستند می‌توانند کشورهای در حال توسعه را وادار کنند که قیمت کالای خود را تا کمترین میزان پایین بیاورند. برخی دولت‌ها اخیراً سازمان‌های طرفدار محیط زیست یا معترضان به تجارت ناعادلانه جهانی را هدف گرفته‌اند.

حتی زمانی هم که هیچ پیامد زیانبار مستقیمی در کار نباشد، صرف وجود یک سیستم نظارت و مراقبت نیرومند می‌تواند اثر وحشتناکی بر آزادی بیان بگذارد و مانع توسعه فرهنگی و سیاسی شود.

همزمان با بحث‌انگیزتر شدن این گونه فعالیت‌ها، ایالات متحده کوشیده است دایره‌ی شرکای خود را گسترش دهد. کشورهای همچون سوئیس و دانمارک اکنون سرگرم ساخت پایگاه‌های ماهواره‌ای جدید برای جمع‌آوری و فروش اطلاعات جاسوسی به ایالات متحده هستند. اما همانگونه که تحقیق‌وتفحص جاری پارلمان اروپا نشان می‌دهد، آگاهی و نگرانی عمومی به سرعت رو به افزایش است. با این حال صرف گوش‌به‌زنگ بودن کافی نیست: اگر قرار است مردم و دولت‌های جهان در زیرساختار جهانی اطلاع‌رسانی حقوق مشترک داشته باشند، باید به سرعت دست به اقدام هماهنگ و مشترک زد. ■

آیا می‌دانستید که...

اشلون می‌تواند روزی ۳ میلیارد پیام ارتباطی(مکالمه تلفنی، نامه الکترونیکی، دریافت فایل از اینترنت، تبادلات ماهواره‌ای و...) و همچنین در هر دقیقه ۲ میلیون تماس تلفنی را شنود کند.

اشلون‌تقریبا۹۰ درصد کل نقل وانتقالات روی اینترنت را وارسی می‌کند.

http://www.echelonwatch.org

برای مطالعه‌ی گزارش پارلمان اروپا، به این پایگاه اینترنتی مراجعه کنید:
www.europarl.eu.int/stoa/publi/default.en.htm

برای کسب اطلاعات بیشتر در مورد شبکه‌های جاسوسی می‌توانید به این پایگاه‌های اینترنتی مراجعه کنید:

ایالات متحده: www.nsa.gov
بریتانیا: www.gchq.gov.uk
کانادا: www.cse.dnd.ca
استرالیا: www.dsd.gov.au
نیوزیلند: www.gcsb.govt.nz
روسیه: www.fsb.ru
آلمان: www.bundesnachrichtendienst.de