
بسم الله الرحمن الرحیم

INDUSTRIAL ESPIONAG
جاسوسی صنعتی

تهیه و تنظیم کنندگان:پورحمزه
گرگری

مقدمه

امروزه پیشرفت درعلم و صنعت و دستیابی به تکنولوژی پیشرفته فقط از طریق محققان ومراکز آموزشی

میسر نیست. استفاده (در واقع سوء استفاده)از تحقیقات و اختراعات دیگران راه ساده استفاده و بی دردسر دستیابی به جدیدترین دستاوردهای تکنولوژیک است ، کاری که در حال حاضر وسعت بسیاری داشته و به جاسوسی صنعتی معروف شده است .

تاریخچه جاسوسی دیجیتا

شاید به نظر برسد جاسوسی و پایش محصول قرن 21 است اما هموار
در تاریخ وجود داشته و قدمت آن را می‌توان با پیدایش تمدن‌ها یکی د
با پیشرفت علم و دانش و ظهور فن‌آوری از دوربین و تلسکوپ و را
تا دوربین‌های مدار بسته، ماهواره‌های جاسوسی، اینترنت، جی‌پی‌اس
روش‌های جاسوسی و پایش بشر نیز دستخوش تحولات و پیچیدگی‌ها
دوران جنگ سرد میان آمریکا و روسیه را می‌توان یکی از مهم‌ترین
و گسترش روش‌ها و ابزار جاسوسی و پایش در تاریخ بشر دانست چ
نظامی کشورهای درگیر، به ندرت به طور مستقیم در جنگ سرد شرک
این نبرد بیشتر توسط آژانس‌های اطلاعاتی مانند سیا آمریکا، MI6 ا
سرویس اطلاعات فدرال آلمان غربی، استاسی آلمان شرقی و کاگب
شوروی انجام می‌شد و به همین دلیل عملیات‌های جاسوسی نیاز دست
اطلاعاتی به ابزار و فن‌آوری‌های جاسوسی و پایش را روز به روز اف
به همین دلیل طرف‌های درگیر سرمایه‌گذاری هنگفتی در پیشرفت تکن
ابداع ابزار و روش‌های جاسوسی و اطلاعاتی کردند. برای نمونه می‌ت
جاسوسی اشلون، سازمان اطلاعاتی مشترک ایالات متحده و انگلستان
جنگ جهانی دوم ایجاد شد و از آن برضد شوروی، چین، و هم‌پیمانان

تاریخچه جاسوسی دیجیتا

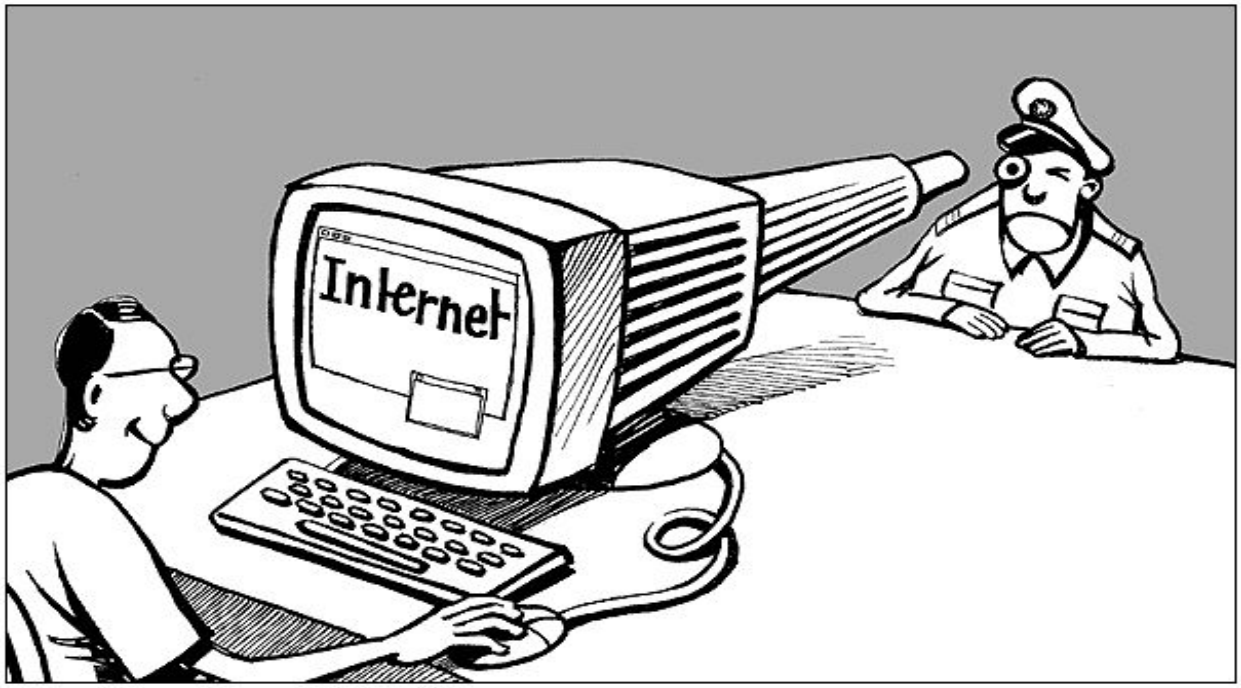
جهان با حملات 11 سپتامبر وارد دوره جدید
از جاسوسی و پایش شد. دولت آمریکا به ب
مردم آمریکا با تصویب قوانین جدید امکان
پایش شدیدتر و جاسوسی از تمامی جنبه‌های
آمریکایی و انجام عملیات‌های جاسوسی در
خود افزایش و هموار کرد. از آن زمان به ب
گسترش فن‌آوری‌های پیشرفته ابزار پیچیده‌ت
پیشرفته‌تر جاسوسی و پایشی نیز ابداع و تو
فن‌آوری‌ها و دستگاه‌هایی که به دست شرکت
آمریکایی که همگی از ارتباط نزدیکی با ساز
اطلاعاتی و نظامی و دولتی این کشور دارند

جاسوسی و پایش اینترنتی

اینترنت به بزرگ ترین **«ماشین جاسوسی و پایش اطلاعات»** جهان تبدیل شده است و این در حالی رخ می‌دهد که به طور روز افزون شاهد این هستیم که اطلاعات شخصي بیشتر افراد نسبت به هر زمان دیگري در اینترنت قرار دارد و آن را به مثابه گنجینه با ارزشی از اطلاعات تبدیل کرده است.

دهه 60 میلادی را می‌توان دهه پیدایش اینترنت نامید. آمریکا با هدف نظارت مجازی بر جهان و پس از ارائه اینترنت در دهه 90 میلادی با گسترش شبکه های اینترنتی در سراسر جهان، میلیاردها نفر را در دام تارهای عنکبوتی سیستم اطلاعاتی خود گرفتار کرد. طبق گزارشی که در سال 2011 منتشر شده در حال حاضر حدود 2 میلیارد و 200 میلیون نفر در جهان از اینترنت استفاده می‌کنند یعنی چیزی حدود یک سوم جمعیت کل جهان.

در واقع هر وسیله‌ای که قابلیت اتصال به اینترنت را داشته باشد از آن می‌توان به عنوان یک جاسوسی و شنود و پایش استفاده کرد.



جاسوسی نو

اطلاعات و جاسوسي بخش خصوصي در حال تبديل شدن به بخش مهمي از نظم نوين اطلاعات جهاني است وقتي از اطلاعات و جاسوسي بحث مي‌شود، معمولاً سازمان‌هاي دولتي مانند سيا، سرويس اطلاعات و جاسوسي انگليس (SIS) و وزارت امنيت ملي چين در ذهن تداعي مي‌شود. اين استنباط عمومي وجود دارد كه اين سازمان‌هاي دولتي هستند كه فعاليت جاسوسي، تجزيه و تحليل اطلاعات و برخي ماموريت‌هاي مختلف را انجام مي‌دهند.

تعدادی از روشهای مهندسی اجتماعی به صورت برنامه
و هدفمند برای دسترسی به اطلاعات مهم و سری یک ش

"جاسوسی صنعتی " عبارت است از به کار گیری همزمان یک یا تعدادی از روشهای مهندسی اجتماعی به صورت برنامه ریزی شده و هدفمند برای دسترسی به اطلاعات مهم و سری یک شرکت .

مطالعات اخیر نشان داده است که افراد داخل یک شرکت ،
مسئول بیش از 70 درصداز دزدیهای اطلاعاتی شرکت بوده اند.

جاسوسی صنعتی ، چرا ؟

دلایل انجام فعالیت های جاسوسی در بخش های صنعتی را می توان موارد ذیل ذکر کرد :

- کسب برتری در مقابل رقیب
- کسب تحقیقات مربوطه با کم ترین هزینه
- کسب فن آوری های جدید صنعتی و نظامی با حداقل هزینه
- کاهش هزینه های پژوهش از طریق کسب دستارودهای دیگران
- کسب اطلاعات در خصوص تحلیل رقبا
- ایجاد سیستم پدافند برای مقابله با خطرات احتمالی

البته مهم ترین هدف جاسوسان ، دست یابی به اطلاعات مراکز فعال در زمینه ی تحقیقات و نتایج آن و همچنین فن آوری های بسیار مدرن است . اینگونه جاسوسی، بیش تر از همه ، موارد و عرصه های زیر را در برمی گیرد :

- صنایع دفاعی و تسلیحاتی
- پردازش اطلاعات وفن آوری ارتباطات الکترونیک
- مواد خام
- فن آوری روند تولید
- بیوتکنولوزی و پزشکی
- انرژی ، حفاظت از محیط زیست
- همکاری فن آورانه و اقتصادی

سلطان جاسوسی صنعتی جهان

در اسناد ديپلماتيك وزارت خارجه آمريكا كه اخيرا توسط "ويكي ليكس" منتشر شده، در اين اسناد از **فرانسه** به عنوان "سلطان سرقت فناوري" سخن به ميان آمده است.

فرانسه در مقياس جهاني، تنها متهم پرونده جاسوسي صنعتي محسوب نمي‌شود بلكه **آمريكا، روسيه، چين، هند و رژيم صهيونيستي** نيز درصدر فهرست متهمين قرار گرفته‌اند. آمريكا در اين زمينه از آلمان و ژاپن، بيشترين سوء استفاده‌هاي ممكن را به عمل آورده و از هر طريق ممكن و تحت پوشش ارتباطات تجاري - خدماتي، در جهت "تخليه اطلاعاتي" مخاطبين عمل مي‌كند. علاوه بر اين، بخش قابل توجهي از اطلاعات موردنظر آمريكا از طريق جاسوسي ماهواره‌اي، شنود ماهواره‌اي و ايستگاههاي استراق سمع تامين وتكميل مي‌شود. علاوه بر اين عمليات جاسوسي و ضد جاسوسي آمريكا از طريق شنود مكالمات تلفني اعم از تلفن‌هاي ثابت و سيار صورت مي‌گيرد

كشورهاي صنعتي بويژه صنايع و شركتهائي كه رقباي فراوان و قدرتمندي دارند، عموما سعي مي‌كنند از "اصل غافلگيري" بهره‌برداري كنند و براي رقباي خود كه كم از دشمن نيستند، "تله‌هاي اطلاعاتي" كار بگذارند و مانع از دستيابي آنها به "اطلاعات هدف" شوند. بعلاوه بعضا با ارائه اطلاعات دستكاري شده، با اشتباهات فني - محاسباتي غيرقابل رديابي،رقيب خود را به راه پرخطا، رهنمون مي‌سازند تا بر اثر كپي‌برداري از اطلاعات و اسناد دستكاري شده، پروژه‌هاي صنعتي مبتني بر جاسوسي، عقيم و غيركارآمد شود.

جاسوسان صنعتی در عرصه ی خود چگونه عمل می کنند ؟

دست یابی به روش های مدیریتی در صنایع به ویژه نظامی از عرصه های خاص فعالیت سرویس های جاسوسی در سراسر جهان محسوب می شود. در این زمینه ، جاسوسان صنعتی معمولاً به موارد ذیل توجه بیشتری از خود نشان می دهند :

- اسناد و اطلاعات مربوط به چارت سازمان ها
- اطلاعات مربوط به برآورد هزینه ها ، بودجه و طرح های سرمایه گذاری
- ایده های جدید در نحوه و نوع تولیدات
- نتایج حاصله از تحقیقات
- مطالعات مربوط به طراحی محصولات نوین
- تدابیر سنجش کیفیت مؤسسات
- روش های مورد استفاده در تأمین نیازهای مشتریان
- استراتژی فروش ،بازاریابی و خرید
- اطلاعات مربوط به اعطای امتیاز و آدرس مشتریان
- مشخصات و آدرس های محققین و صاحبان تخصص و ...

روشهای جاسوسی صنعتی

- **روشهای قانونی:**

1)خرید شرکت ها یا محصولاتشان که سبب انتقال تکنولوژی به رقبای سابق شرکت خریداری شده است

2)انتقال تکنولوژی به کشورهای دیگر از راه انجام تجارت در آنها که ضمن آن شرکت مجبور میشود ابتدا نیروی انسانی خارجی را آموزش دهد

3)انجام کار مشترک با سایر رقبا؛در واقع به اشتراک گذاری اطلاعات

4)اطلاعات منبع باز :مانند روزنامه ها ،مقالات ،گزارشهای سالانه شرکت و...

5)استخدام کارکنان توسط شرکت های دیگر و رقبا

6) کنفرانس ها و برنامهای تبلیغاتی

روشهای غیر قانونی

1. سوءاستفاده از افراد داخلی برای دزدیدن اطلاعات چه به صورت آگاهانه (مثل تطمیع کارکنان)و چه به صورت نا آگاهانه مانند تلفن کردن
2. فرستادن جاسوسهایی به شرکت در قالب افراد واجد تخصص و جویای کار
3. حمله فیزیکی به شرکت
4. سایر روشها از جمله گشتن اتاق نمایندگان در هتل و یا تخلیه اطلاعاتی افراد مطلع

تفاوت جاسوسی بخش صنعتی ودولتی

- هدف اطلاعات و جاسوسي دولتي حفاظت از كشور است، در حالي كه هدف اصلي اطلاعات و جاسوسي بخش خصوصي عمدتاً كسب سود اقتصادي بيشتر است.

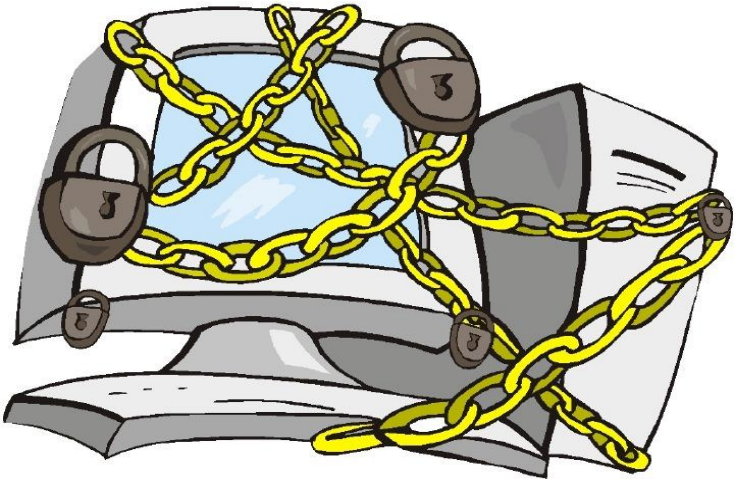
- يكي ديگر از تفاوت‌هاي اطلاعات بخش خصوصي و دولتي در اين است كه سازمان‌هاي اطلاعاتي دولتي، بخشي مستقل هستند و قسمتي از زيرساختار دولت محسوب مي‌شوند.

اما فعاليت اطلاعاتي بخش خصوصي به صورت مستقل دنبال نمي‌شود.

تفاوت جاسوسی بخش صنعتی ودولتی

هدف از جاسوسي در بخش خصوصي كسب سود اقتصادي از طريق فروش اطلاعات حساس به مشتريان است. عمده اين مشتريان خود شركت‌هايي هستند كه از طريق دستيابي به اين اطلاعات سعي در كسب سود اقتصادي بيشتر دارند.

راهای جلوگیری از جاسوسی صنعتی



- **امنیت فنی؛** مانند نصب دیوارهای مخصوص
- **امنیت عملی؛** شناسایی قسمت هایی که امکان نشت اطلاعات از آن وجود داردو بکارگیری سیاستهاو قوانین متناسب.
- **امنیت فیزیکی؛** دسترسی به دارایی های شرکت باید توسط قفل ها ،نگهبان ها و دستگاههای تشخیص هویت کنترل شود.
- **امنیت شخصی؛** سوابق افراد شاغل به دقت بررسی شود بخصوص مشاغل سطح پایین که در معرض خطر بیشتر و از سطح سواد پایین تری برخوردارند.

راه های مقابله با جاسوسی صنعتی

- ✔ تعریف و مشخص کردن بخش های حساس
- ✔ تعیین اطلاعاتی که نیازمند مراقبت گسترده هستند .
- ✔ مشخص کردن افرادی که اجازه دسترسی به اطلاعات محرمانه را دارند .
- ✔ تعیین وظایف بخش های مختلف سازمان در ارتباط با حفاظت از داده ها
- ✔ ارائه تعریفی یکسان از روش های کاری ایمن در برابر جاسوسی
- ✔ اتخاذ تدابیر امنیتی فنی و سازمانی به منظور مراقبت از این اطلاعات ارزشمند و محرمانه

چشم انداز آینده

اگرچه تلاش‌های غرب برای جاسوسی از مردم و به ویژه ایران به طور روزافزون ابعاد تازه‌ای به خود می‌گیرد اما می‌توان با اتخاذ تدابیری این حفره‌های امنیتی را مسدود کرد. اگرچه امنیت هرگز ۱۰۰ درصدی نخواهد بود اما با راهبردهای کارشناسی شده و آموزش می‌توان از وقوع جاسوسی و حملات دیجیتالی و سایبری جلوگیری کرد. استفاده از نرم افزارهای امنیتی جدید و به روز، آموزش همگانی و اطلاع رسانی در مورد خطرات و تهدیدهای موجود در اینترنت و ....، جلوگیری از مهندسی اجتماعی برای انجام عملیات جاسوسی سایبری، تشکیل پلیس اینترنتی و فضای سایبر و به کارگیری از اینترنت ملی می‌توانند از بهترین رویکردها برای مقابله با جاسوسی عصر نوین در حال حاضر باشند.

تعدادی از ابزار قدیمی جاسوسی

رژ لب مرگبار

این یک اثر کلاسیک جاسوسی است. رژ لبی که می تواند یک گلوله میلیمتری 4.5 شلیک کند. این اسلحه در اواسط سال 1960 KGB به دست امده از یک مامور است. و هم اکنون در موزه بین المللی ابزارهای جاسوسی نگهداری میشود

اما این دوربین چهل سال قبل یکی از بهترین دوربین ها برای عکاسی مخفیانه بوده. دوربین در کت جاسازی میشده

و جاسوس می توانست به راحتی با آن عکاسی کند.

لباس عکاس

این روزها دوربین موبایل شما خیلی کوچک تر از این دوربین جاسوسی است. اما این دوربین چهل سال قبل یکی از بهترین دوربین ها برای عکاسی مخفیانه بوده. دوربین در کت جاسازی میشده و جاسوس می توانست به راحتی با آن عکاسی کند.

یک پایگاه نظامی هوایی روسی نزدیک را دریافت می کرد و آنها را به یک ماهواره آمریکایی ارسال می کرد. جالب تر اینکه این دستگاه با انرژی خورشیدی کار می کرد! بنابراین نیازی به نگهداری و تعویض باطری نداشت.

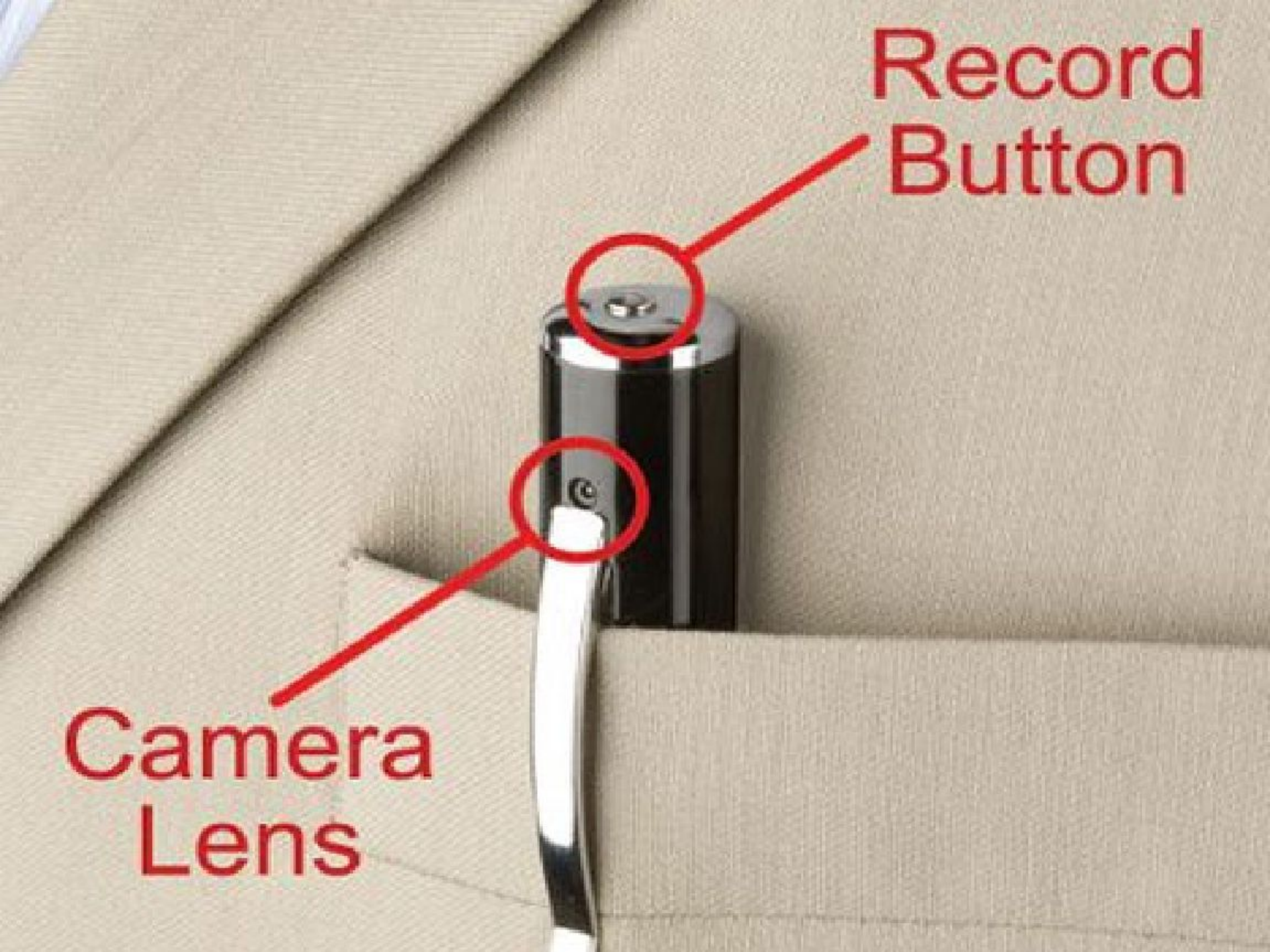
درخت جاسوس

روس ها در سال 1970 در جنگل های اطراف مسکو درون تنه یک درخت این گیرنده و فرستنده را کشف کردند! امریکایی ها آن را در آنجا جاسازی کرده بودند. این دستگاه پیام های رادیویی از یک پایگاه نظامی هوایی روسی نزدیک را دریافت می کرد و آنها را به یک ماهواره آمریکایی ارسال می کرد. جالب تر اینکه این دستگاه با انرژی خورشیدی کار می کرد! بنابراین نیازی به نگهداری و تعویض باطری نداشت.

ترجیح می داند لباس هایشان را از غرب و از طریق پست بخرند. در رومانی سرویس جاسوسی از این موضوع استفاده می کرد و با هماهنگی شرکت پست، در پاشنه کفش هایی که آنها میخریدند ردیاب و میکروفن مخفی جاسازی می کرد. این کفش به طور اتفاقی در طی یک بررسی امنیتی در یک سالن کشف شد. ماموران یک سیگنال در سالن کشف کردند اما وقتی دیپلمات ها سالن را ترک می کردند سیگنال ناپدید میشد!

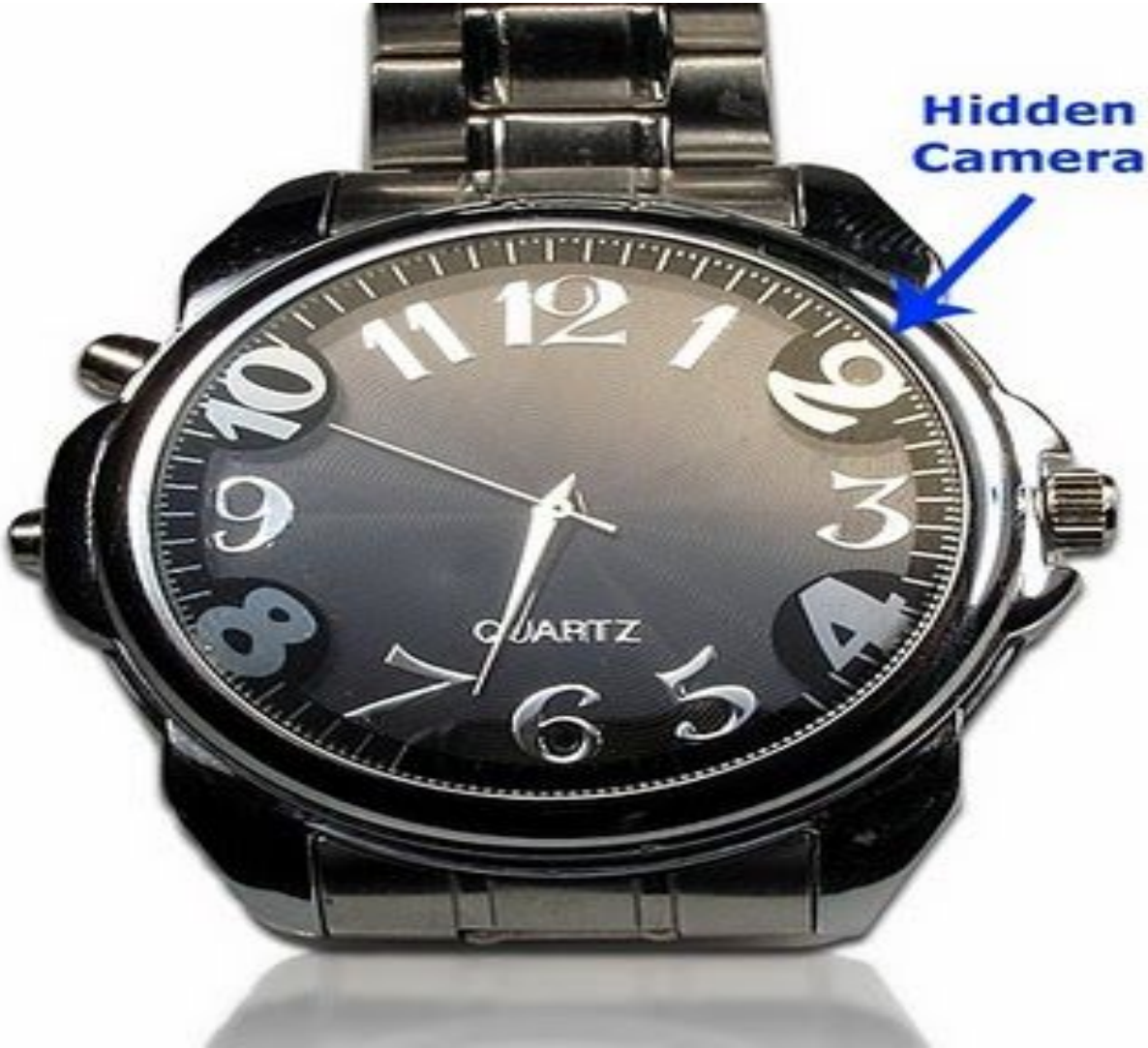
بین سال های ۶۰ و ۷۰ میلادی اکثر دیپلمات های غربی که در شرق اروپا مشغول کار بودند ترجیح می داند لباس هایشان را از غرب و از طریق پست بخرند. در رومانی سرویس جاسوسی از این موضوع استفاده می کرد و با هماهنگی شرکت پست، در پاشنه کفش هایی که آنها میخریدند ردیاب و میکروفن مخفی جاسازی می کرد. این کفش به طور اتفاقی در طی یک بررسی امنیتی در یک سالن کشف شد. ماموران یک سیگنال در سالن کشف کردند اما وقتی دیپلمات ها سالن را ترک می کردند سیگنال ناپدید میشد!

ابزارهای جدید جاسوسی


Record
Button
Camera
Lens


Camera


Record
zero
zero
On / OFF
Power Switch


Hidden
Camera
QUARTZ


BITRONIC.IR

با سپاس از
توجه تان

اسفند 1391