

سلامت و سلامتی



INDUSTRIAL ESPIONAG

جاسوسی صنعتی

تہیہ و تنظیم کنندگان: پور حمزہ
گرگری



مقدمه

امروزه پیشرفت در علم و صنعت و دستیابی به تکنولوژی پیشرفته فقط از طریق محققان و مراکز آموزشی

میسر نیست. استفاده (در واقع سوء استفاده) از تحقیقات و اختراعات دیگران راه ساده استفاده و

بی دردسر دستیابی به جدیدترین دستاوردهای تکنولوژیکی است ، کاری که در حال حاضر وسعت

بسیاری داشته و به جاسوسی صنعتی معروف شده است .



تاریخچه جاسوسی دیجیتال

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 با پیشرفت علم و دانش و ظهور فن‌آوری از دوربین و تلسکوپ و راد 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 شرکت این نبرد بیشتر توسط آژانس‌های اطلاعاتی مانند سیا آمریکا، MI6 از 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 افزایش داد به همین دلیل طرف‌های درگیر سرمایه‌گذاری هنگفتی در پیشرفت تکنولوژی ابداع ابزار و روش‌های جاسوسی و اطلاعاتی کردند. برای نمونه می‌توان به جاسوسی اشلون، سازمان اطلاعاتی مشترک ایالات متحده و انگلستان در جنگ جهانی دوم ایجاد شد و از آن برضد شوروی، چین، و همپیمانان





تاریخچه جاسوسی دیجیتال

جهان با حملات 11 سپتامبر وارد دوره جدید از جاسوسی و پایش شد. دولت آمریکا به 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 دسترس فن‌آوری‌های پیشرفته ابزار پیچیده‌تر 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

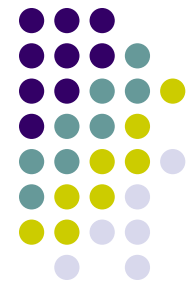




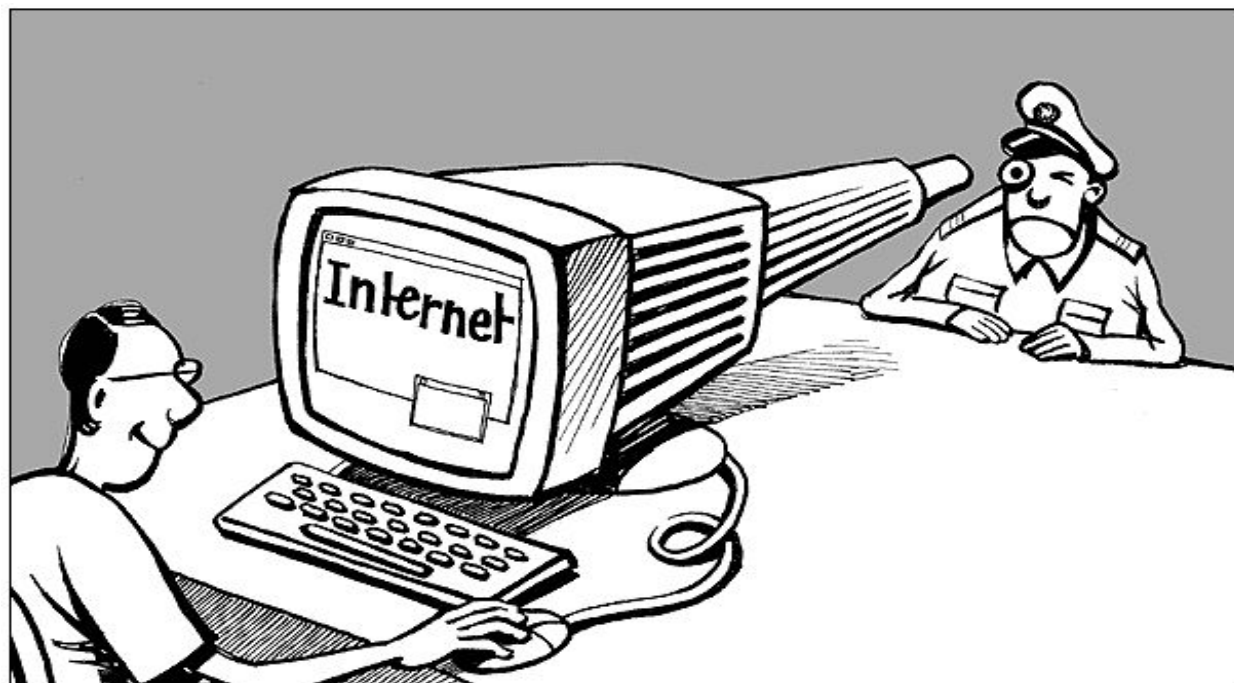
جاسوسی و پایش اینترنتی

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 شخصی بیشتر افراد نسبت به هر زمان دیگری 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 ایند را داشته باشد از آن می‌توان به عنوان یک جاسوسی و شنود و پایش استفاده کرد.





جاسوسی نو

اطلاعات و جاسوسی بخش خصوصی در حال تبدیل شدن به بخش مهمی از نظم نوین اطلاعات جهانی است. وقتی از اطلاعات و جاسوسی بحث می‌شود، معمولاً سازمان‌های دولتی مانند سیا، سرویس اطلاعات و جاسوسی انگلیس (SIS) و وزارت امنیت ملی چین در ذهن تداعی می‌شود. این استنباط عمومی وجود دارد که این سازمان‌های دولتی هستند که فعالیت جاسوسی، تجزیه و تحلیل اطلاعات و برخی مأموریت‌های مختلف را انجام می‌دهند.



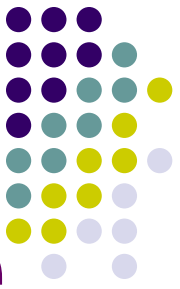
تعدادی از روشهای مهندسی اجتماعی به صورت برنامه و هدفمند برای دسترسی به اطلاعات مهم و سری یک ش



“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 درصد از 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 دستاوردهای 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 بر می گیرد :


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



سلطان جاسوسی صنعتی جهان

در اسناد دیپلماتیک وزارت خارجه آمریکا که اخیرا توسط "ویکی لیکس" منتشر شده، در این اسناد از **فرانسه** به عنوان "سلطان سرقت فناوری" سخن به میان آمده است.

فرانسه در مقیاس جهانی، تنها متهم پرونده جاسوسی صنعتی محسوب نمی‌شود بلکه **آمریکا، روسیه، چین، هند و رژیم صهیونیستی** نیز در صدر فهرست متهمین قرار گرفته‌اند. آمریکا در این زمینه از آلمان و ژاپن، بیشترین سوء استفاده‌های ممکن را به عمل آورده و از هر طریق ممکن و تحت پوشش ارتباطات تجاری - خدماتی، در جهت "تخلیه اطلاعاتی" مخاطبین عمل می‌کند. علاوه بر این، بخش قابل توجهی از اطلاعات موردنظر آمریکا از طریق جاسوسی ماهواره‌ای، شنود ماهواره‌ای و ایستگاه‌های استراق سمع تامین و تکمیل می‌شود. علاوه بر این عملیات جاسوسی و ضد جاسوسی آمریکا از طریق شنود مکالمات تلفنی اعم از تلفن‌های ثابت و سیار صورت می‌گیرد.



کشورهای صنعتی بویژه صنایع و شرکتهایی که رقبای فراوان و قدرتمندی دارند، عموماً سعی می‌کنند از "اصل غافلگیری" بهره‌برداری کنند و برای رقبای خود که کم از دشمن نیستند، "تله‌های اطلاعاتی" کار بگذارند و مانع از دستیابی آنها به "اطلاعات هدف" شوند. بعلاوه بعضاً با ارائه اطلاعات دستکاری شده، با اشتباهات فنی - محاسباتی غیرقابل ردیابی، رقیب خود را به راه پرخطا، رهنمون می‌سازند تا بر اثر کپی‌برداری از اطلاعات و اسناد دستکاری شده، پروژه‌های صنعتی مبتنی بر جاسوسی، عقیم و غیرکارآمد 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 برنامههای 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 و دولتی

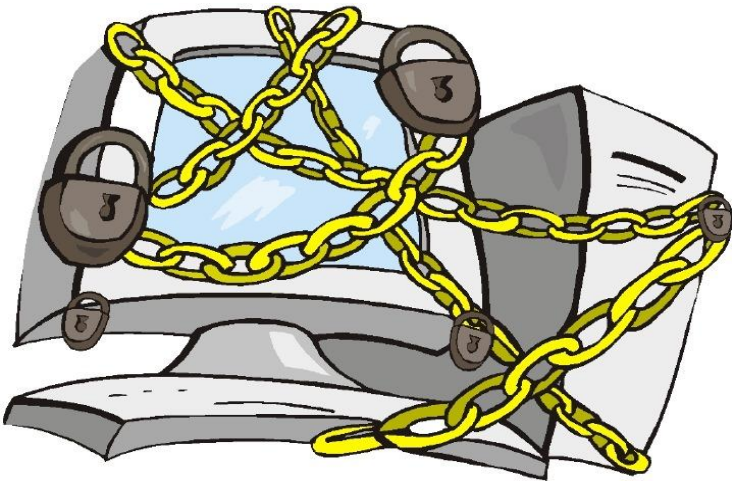
هدف اطلاعات و جاسوسی دولتی حفاظت از کشور است، در حالی که هدف اصلی اطلاعات و جاسوسی بخش خصوصی عمدتاً کسب سود اقتصادی بیشتر است.

یکی دیگر از تفاوت‌های اطلاعات بخش خصوصی و دولتی در این است که سازمان‌های اطلاعاتی دولتی، بخشی مستقل هستند و قسمتی از زیرساختار دولت محسوب می‌شوند. اما فعالیت اطلاعاتی بخش خصوصی به صورت مستقل دنبال نمی‌شود.

تفاوت جاسوسی بخش صنعتی و دولتی

هدف از جاسوسی در بخش خصوصی کسب سود اقتصادی از طریق فروش اطلاعات حساس به مشتریان است. عمده این مشتریان خود شرکت‌هایی هستند که از طریق دستیابی به این اطلاعات سعی در کسب سود اقتصادی بیشتر دارند.

راه‌های جلوگیری از جاسوسی صنعتی



امنیت فنی؛ مانند نصب دیوارهای مخصوص
امنیت عملی؛ شناسایی قسمت هایی که امکان
نشت اطلاعات از آن وجود دارد و بکارگیری
سیاستها و 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
به خصوص 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 به دست امده KGB 1960 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 باتری نداشت.



درخت جاسوس

روس ها در سال 1970 در جنگل های اطراف مسکو درون تنه یک درخت این گیرنده و فرستنده را کشف کردند! آمریکایی 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 باتری 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

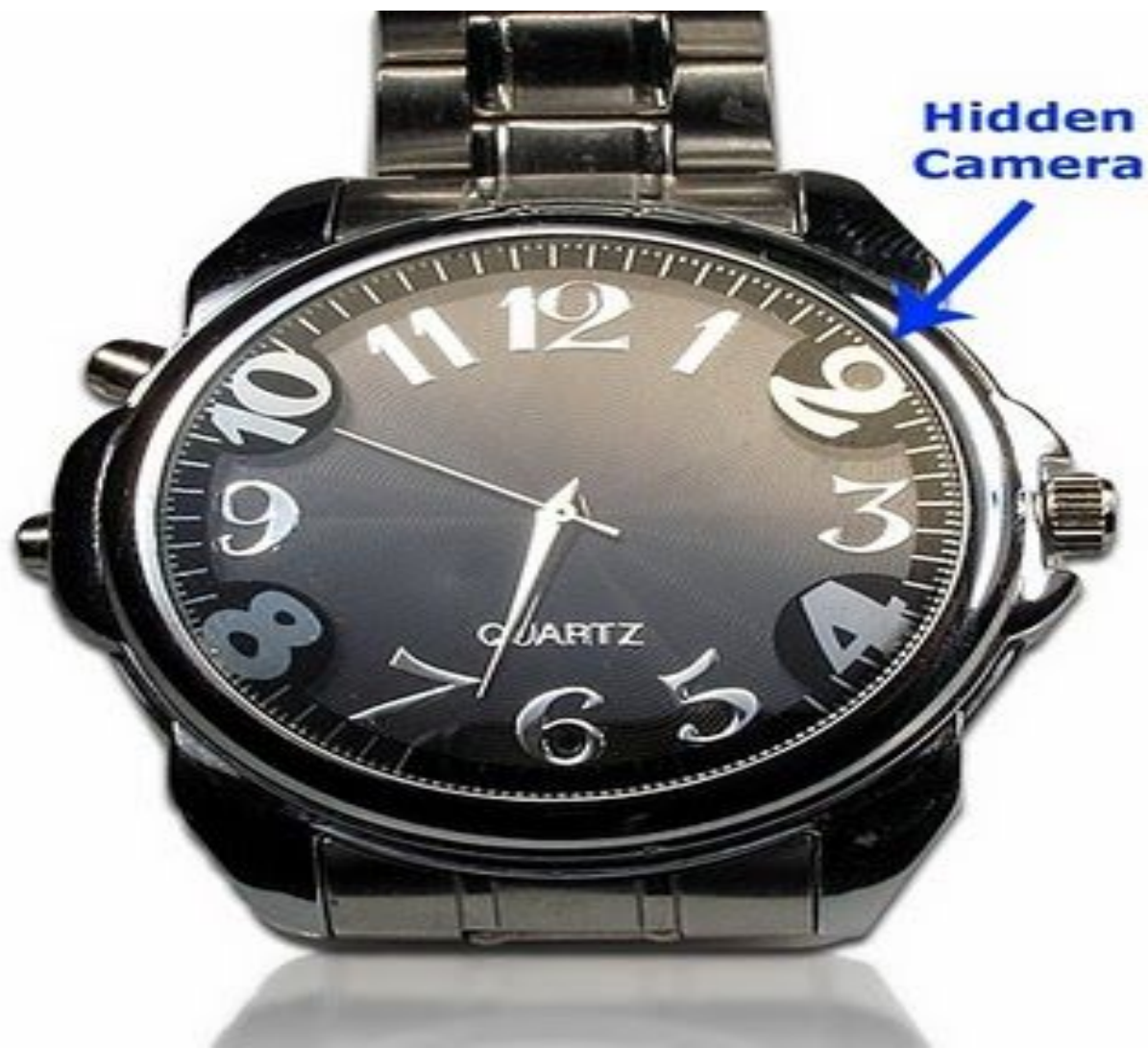


On / OFF

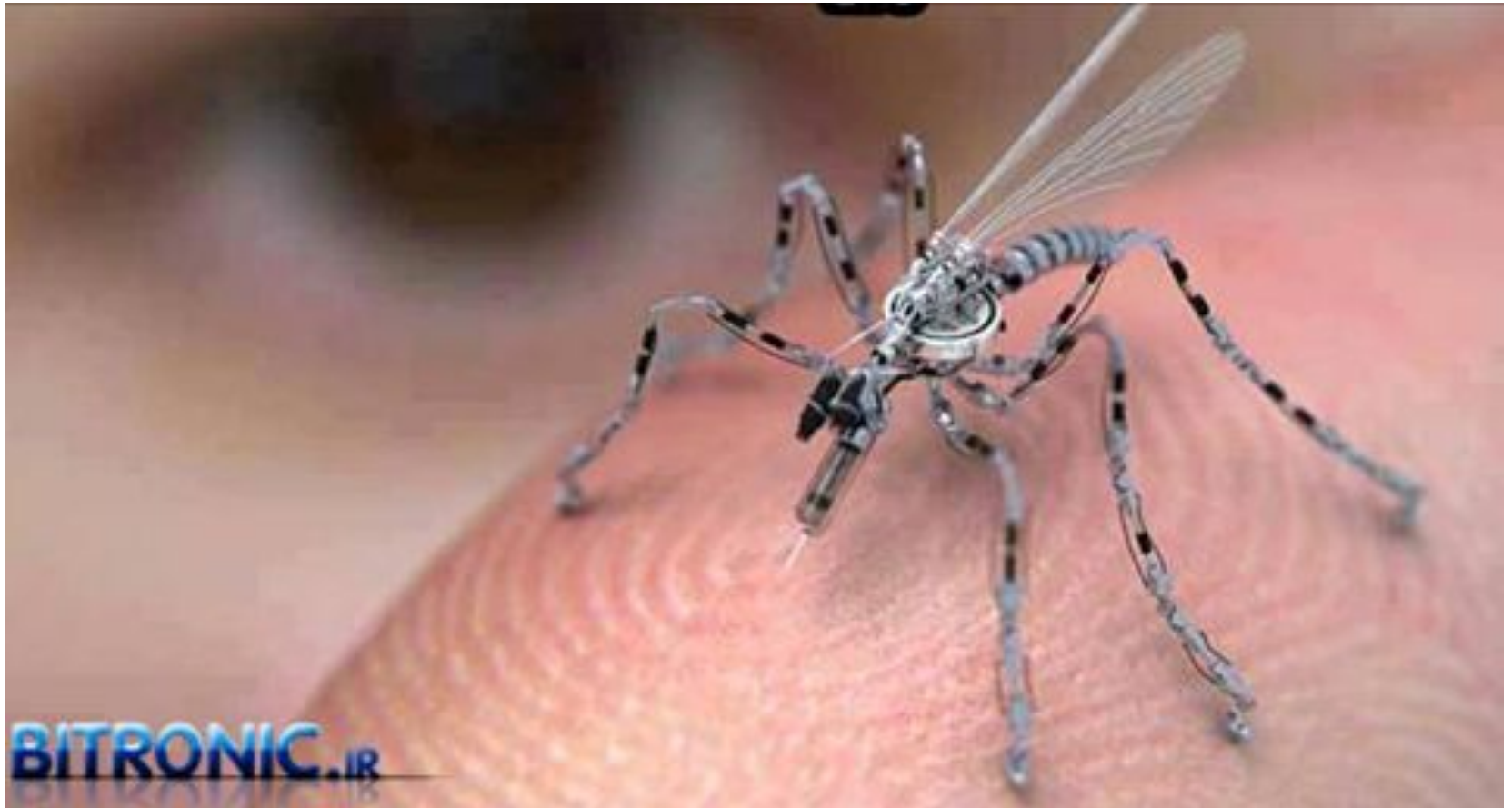


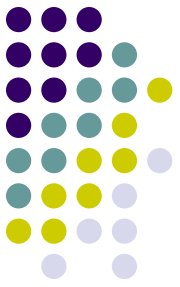
Power Switch





**Hidden
Camera**







با سپاس از توجه تان

اسفند 1391