طه الراوي | نشر في ٢٨ فبراير ,٢٠٢٠

كيف غيرت التكنولوجيا أساليب التجسس؟

التجسس؟ أساليب التكنولوجيا غيرت كيف · بودكاست نون NoonPodcast

في الماضي، كان نشاط التجسس يوجه نحو الحصول على معلومات سياسية وعسكرية فقط، لكن في عالم اليوم الذي تحركه التكنولوجيا، فإن متطلبات الاستخبارات في عدد من الدول باتت أوسع من ذي قبل، وتشمل الآن تقنيات الاتصالات وتكنولوجيا المعلومات والطاقة والبحث العلمي والدفاع والطيران والإلكترونيات والعديد من المجالات الأخرى.

تاريخ التجسس في الدفاع

تُعدّ الجاسوسية مهنة من أقدم المهن التي مارسها الإنسان داخل المجتمعات البشرية منذ فجر الخليقة، فكانت تدفعه إليها غريزته الفطرية للحصول على المعرفة ومحاولة استقراء المجهول وكشف أسراره التي قد تشكل خطرًا يترصد به في المستقبل.

لذلك تنوعت طرق التجسس بدءًا من الاعتماد على الحواس المجردة والحيل البدائية والتقديرات التخمينية، وانتهاءً بالثورة التكنولوجية في ميدان الاتصالات والمعلومات.

وكان أقدم من لجأ إلى هذه الآلية هم جيوش الصين والهند، فقد استخدموا العملاء السريين وقاموا بالاغتيالات، كما نظم المصريون القدماء عمليات التجسس تنظيمًا دقيقًا ومثال ذلك الملك تحتمس الثالث فرعون مصر الذي نظم أول جهاز مخابرات عرفه العالم.

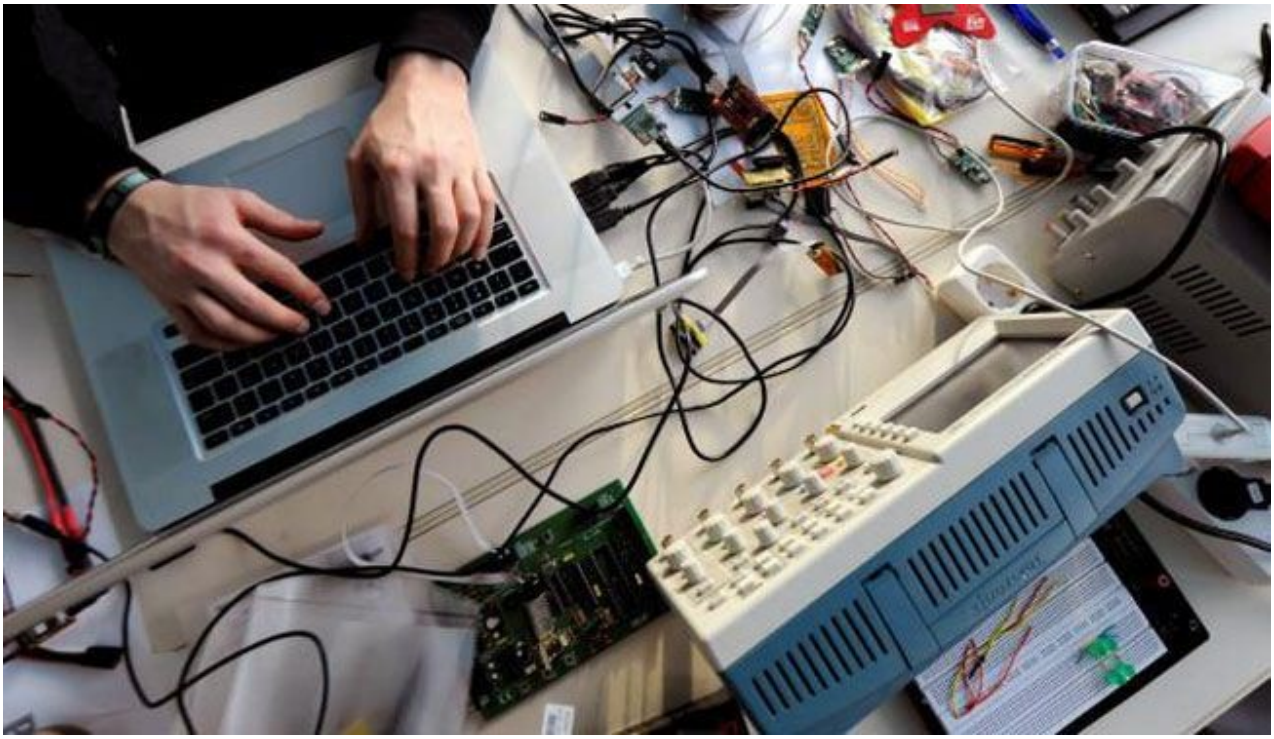
العبرانيون أيضًا استخدموا الجواسيس، وكان نظام الجواسيس سائدًا في الإمبراطوريات اليونانية والرومانية خلال القرنين الثالث عشر والرابع عشر، واعتمد المغول اعتمادًا كبيرًا على التجسس في توغلهم في آسيا وأوروبا، وكانت اليابان غالبًا ما تستخدم النينجا لجمع المعلومات الاستخباراتية.

مهنة التجسس والمجتمع

تختلف ممارسة التجسس بين مجتمع وآخر حسب نوع الأعراف والتقاليد، فنراه على سبيل المثال سمة ثابتة عند اليابانيين، حتى إن الجار يتجسس على جاره بلا حرج، كما أن الشعب الياباني يؤمن بأن العمل

في مجال المخابرات خدمة نبيلة، في حين أن معظم شعوب العالم تستحقر هذه المهنة التي لا غنى عنها في الدولة المعاصرة لتؤدي مسؤولياتها، فلا يكفي أن تكون الدولة كاملة الاستعداد للحرب في وقت السلم، بل لا بد لها من معلومات سريعة كافية لتحمي نفسها وتحقق أهدافها في المعترك الدولي.

أصبح جهاز المخابرات الضمان الأساسي للاستقلال الوطني، كما أن غياب جهاز مخابرات قوي يعني فشل القوات العسكرية في الحصول على إنذار سريع، كما أن اختراق الجواسيس لصفوف العدو يسهل هزيمته.



الاستخبارات والتجسس

تقوم الحرب الإلكترونية والتجسس الإلكتروني على أساس سرقة معلومات العدو أو الحصول على منفذ للتسلل إلى حواسيب العدو وأخذ معلوماته وكذلك تدمير نظم وحواسيب العدو وتعطيلها وتخريب أنظمتها.

تعتبر برامج الاختراق والتجسس الإلكتروني من نتائج الشركات المرتبطة بالاستخبارات العالمية المحترفة، وكذلك جميع ما ينتج من فيروسات لأغراض التدمير الإلكتروني هي الأخرى من نتاج الاستخبارات.

"إسرائيل" الأولى عالميًا في التجسس الإلكتروني

تعتبر "إسرائيل" الأولى عالميًا في عمليات التجسس الإلكتروني وتمتلك 27 شركة متخصصة في هذا المجال، والغريب أن أمريكا وبريطانيا وفرنسا وروسيا والصين لا تمتلك مجتمعة هذا العدد.

حيث تمتلك "إسرائيل" وحدة 8200 لتنفيذ الحرب الإلكترونية والتجسس الإلكتروني، وعند تقاعد خبراء هذه الوحدة الفنية عالية التدريب يتم اجتذاب شخوصها إلى الشركات الإسرائيلية المختصة في هذا المجال لتدريبهم مجموعات جديدة.

أهم وأحدث أجهزة التجسس في الدفاع

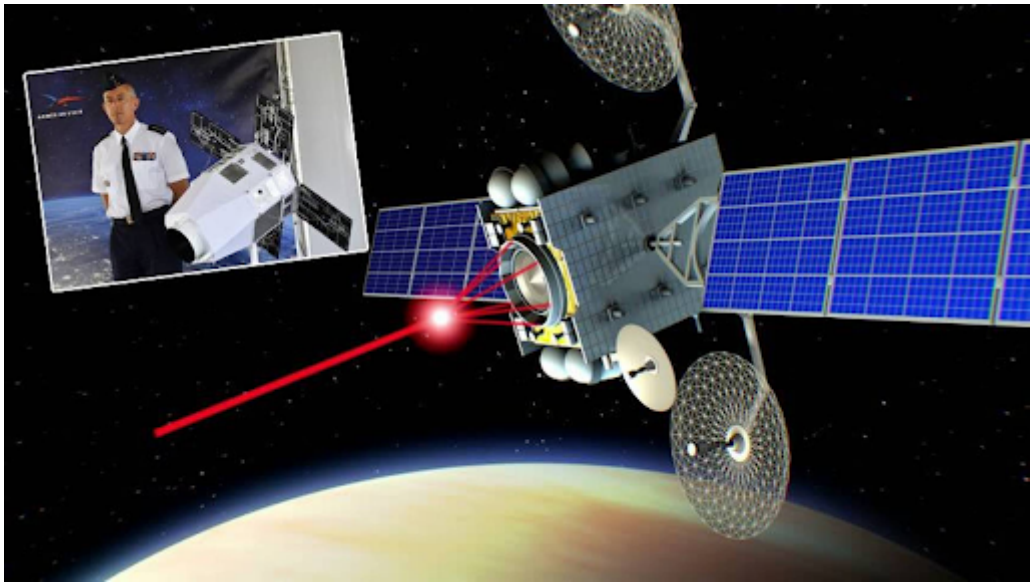
تتنوع الأدوات والتقنيات المستخدمة لأغراض التجسس العسكري، وأهمها:

أقمار التجسس تغزو الفضاء

500 قمر صناعي عسكري تابع للدول العظمى تراقب الأرض لـ24 ساعة، أمريكا تمتلك 50 منها، تكلفتها ليست مرتفعة وأقصى فترة عمل لها سنة.

"قمرنا مدني وليس عسكريًا" هي عبارة ترددها العديد من الدول عند إطلاق أقمار صناعية لتوهم العالم بأن أغراض أقمارها مدنية وتستخدمها داخل حدودها ولن تتجسس بها على الدول الأخرى، لأن القوانين تحظر إطلاق أقمار صناعية عسكرية للتجسس في الفضاء.

إن قمر التجسس يستخدم في حالة الحروب بين الدول، حيث تستخدم بعض الدول أكثر من قمر في الوقت ذاته لمراقبة أعدائها على مدار 24 ساعة والتعرف على ما يمتلكون من إمكانات وما يعدون للحرب.



ساعة حائط

من أشهر أساليب التجسس هي ساعة الحائط حيث تحتوي على كاميرا مخفية وتعمل بتقنية 3G، مزودة ببطارية ذات عمر طويل.

يمكن الاتصال بها عبر شريحة مزودة بها والاستماع إلى التسجيلات، كما يمكن أن تستقبل رسائل نصية لتفعيل عملها وبدء التسجيل أو الإيقاف، وبها إمكانية التسجيل بشكل مباشر إلى ذاكرة تخزين SD ويمكن وضع ذاكرة بحجم 32 جيجا بايت.

كذلك يمكن بث تسجيل مباشر والاستقبال بواسطة هاتف android ومتابعة ما يجري. هناك الكثير من هذه الأجهزة مثل أجهزة على شكل قلم أو ساعة يد أو ميدالية مفتاح سيارة شبيهة بجهاز الريموت للسيارات وغيرها.

أجهزة البوليمرات

هذه الأجهزة مصنوعة من مادة من نوع خاص من "البوليمرات"، ابتكرها باحثون في الجمعية الكيميائية الأمريكية، يمكن أن تدمر نفسها ذاتيًا وتختفي من دون ترك أي أثر بعد أداء مهمتها السرية.

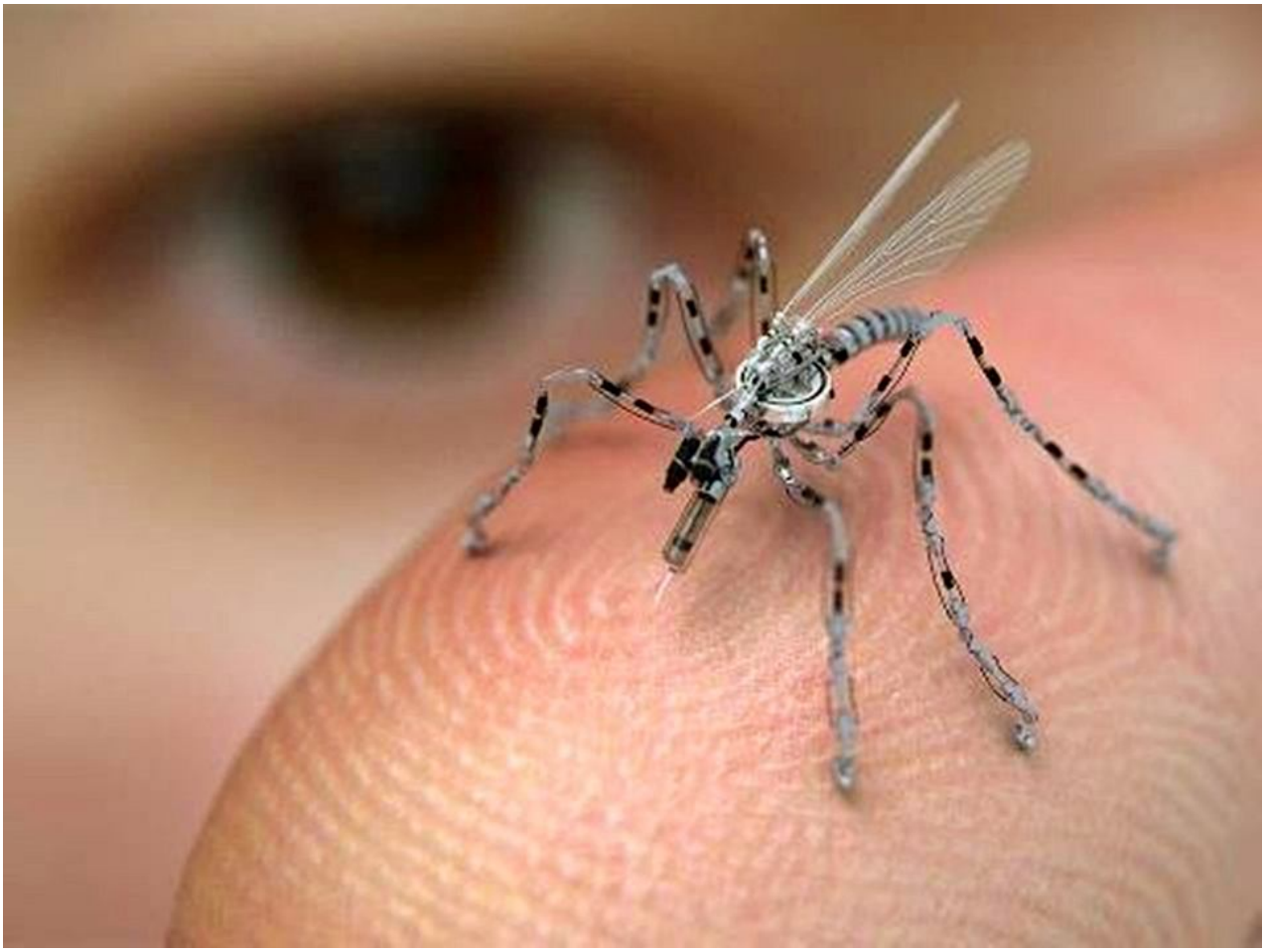
يمكن استخدامها لتصنيع أجهزة الاستشعار والتجسس الإلكترونية، تُلقى في أرض العدو للاستطلاع وتخزين المعلومات قبل تدمير نفسها والاختفاء كأنها لم تكن موجودة من الأساس.

هذه المادة لا تتحلل ببطء على مدار عام، مثل المواد البلاستيكية القابلة للتحلل، بل يختفي هذا "البوليمر" في لحظات عندما يتلقى أمر التدمير الذاتي.

ذبابة استخباراتية

هي ذبابة روبوتية عرضها 3 سنتيمترات فقط قادرة على الطيران والهبوط على أي جسم مع وجود نافذة صغيرة فيها لسحب عينة من الحمض النووي للشخص المستهدف أو إجراء مسح بالأشعة فوق البنفسجية له دون علمه.

كذلك هي مزودة بالكاميرات والميكروفونات التي تسمح بنقل الصوت والصورة بشكل حيّ ومُباشر مثل الذبابة المجندة درون (Drone).



قناديل بحر تجسسية

عبارة عن روبوت آلي مرتبط بمادة مطاطية مرتبطة بجزيئات مغناطيسية تسمح لها بالحركة أو السباحة، تقلد حركة قنديل البحر وتقوم بالتجسس البحري على حركة أساطيل العدو والملاحة والتقاط إشارات تحركهم وتوجههم.

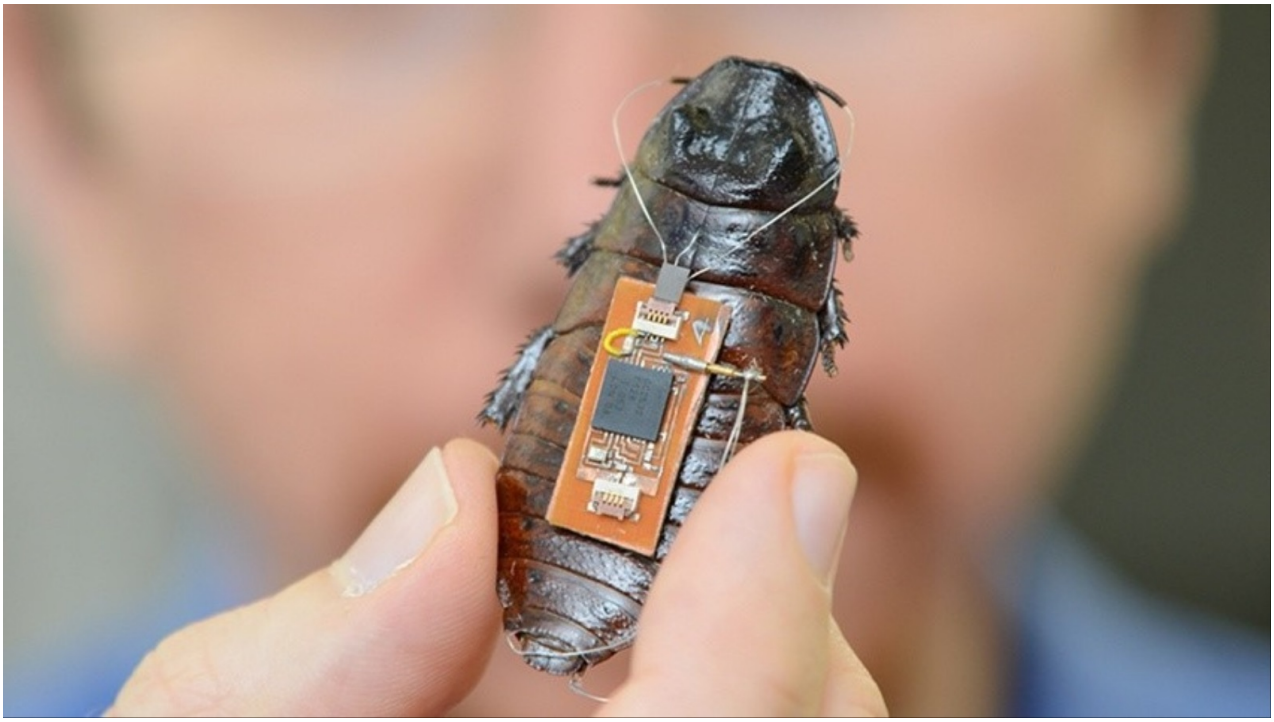
تقنية البايو بت BioBot

يقصد بها الاستفادة مما هو موجود في الحياة الطبيعية وتطعيمه تقنيًا لتنفيذ مهام مختلفة يمكن للبشرية الاستفادة منها، ليخرج عن ذلك ما يُعرف بالأحياء الآلية "بايو بوت"، فهي كائنات حية مسيرة إلكترونيًا، أي أن أدمغتها مرتبطة بتقنيات وخوارزميات لتنفيذ مهام متنوعة منها:

الصرصار الجاسوس

"هوانغ ليانغ" (Liang Hong) باحثة في جامعة تكساس وقع اختيارها على الصراصير القادمة من أمريكا اللاتينية لكونها متوافرة بكثرة وأجسامها قادرة على التعافي بسرعة، إضافة لكونها كبيرة الحجم وبطيئة الحركة، وهذا يجعلها مناسبة لحمل حقيبة مزودة بتقنيات يمكن الاستفادة منها في أكثر من مجال تجسسي.

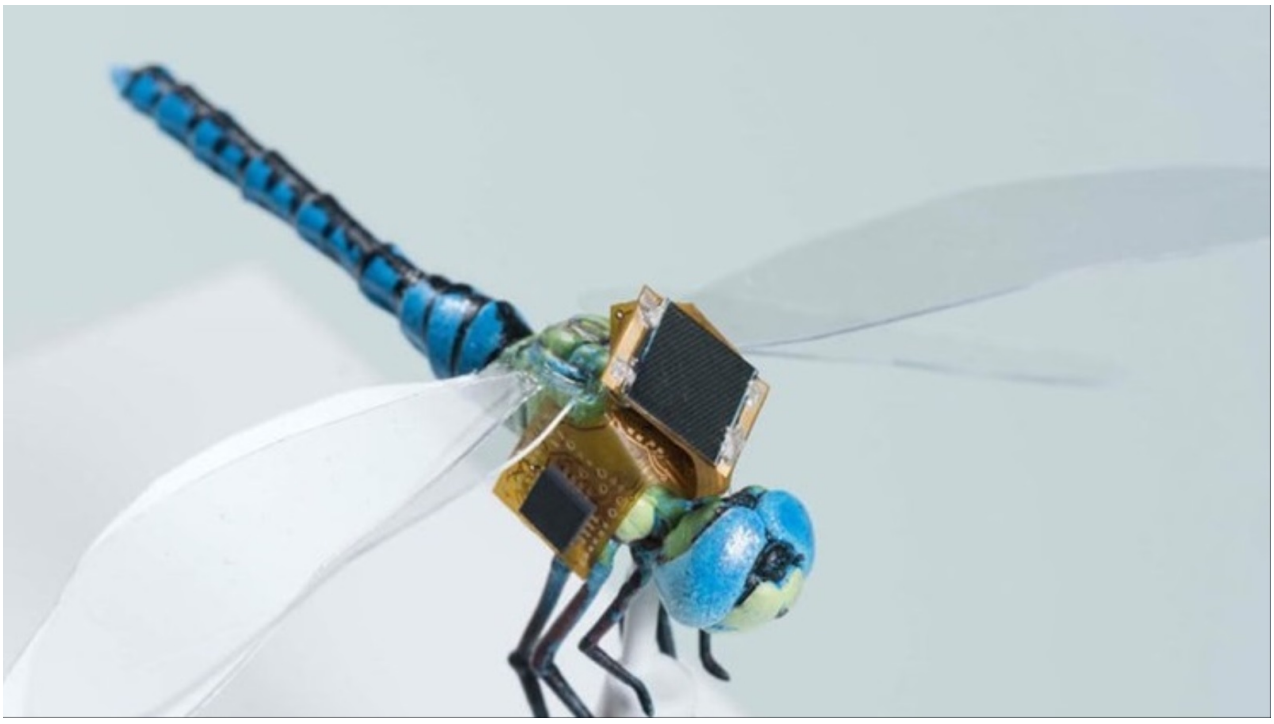
ومن هنا، فإن استخدامات الصرصار الآلي مُتعددة تبدأ من إطلاقه في حالات الطوارئ للوصول إلى المصابين المدفونين تحت الأنقاض على سبيل المثال، وصوًلا إلى مخازن الأسلحة والمواد الممنوعة للتجسس على الحوارات التي تجري وشن حملات مداهمة بحق أصحابها، وفي أسوأ الحالات، قد تكون وسيلة فعالة لمراقبة المواطنين.



اليعسوب التجسسي

يستخدم اليعسوب في التجسس ويساعده بذلك وجود عضلات أسفل أجنحته مسؤولة عن تحريكه خلال الطيران.

باستخدام التيار الكهربائي يُمكن دفع اليعسوب إلى الطيران والهبوط أو حتى الاتجاه إلى اليمين أو اليسار في أثناء الطيران دون القلق من اختلال توازنه لأنها ستحافظ عليه دون مشاكل.



نظارات تجسس ذكية

هي نظارات ذكية مزودة بكاميرات للتعرف على هوية الأشخاص، فبمجرد النظر للشخص تظهر هويته التعريفية المسجلة، مرتبطة بقاعدة بيانات مخزنة في السحابة، وخلال أجزاء من الثانية يستلم مرتدو النظارة معلومات كاملة عن الشخص المطلوب، يرتديها رجال الشرطة في المطارات ومحطات القطار.

سري للغاية

هناك الكثير من الأجهزة التجسسية، ولكن من يعتقد أن المؤسسات العسكرية سوف تتفاخر في العلن بأحدث تقنياتها مثل الشركات التقنية فهو مُخطئ، فهذا التفاخر يعني أن تلك التقنيات أصبحت جزءًا من الماضي وما خفي أعظم بكل تأكيد، لأن واقع المؤسسات وتحديدًا العسكرية، تصنف أي مشروع على أنه سري للغاية للاستفادة منه في المجالات العسكرية المختلفة ولن تُفصح عنه أبدًا.

وهذا يعني أن الأبحاث التي تطفو على السطح الآن قد تكون جزءًا بسيطًا جدًا من أبحاث أكبر تجري في المُختبرات لتكون جاهزة للتطبيق العسكري، وهذا ما ذكرته مُستندات "ويكيليكس" (WikiLeaks) التي أظهرت أجهزة مختلفة للتجسس، بعضها توقفت الوكالات الأمنية عن استخدامه، وبعضها الآخر بقي مستخدمًا حتى تسريب المستندات، لتلجأ تلك الهيئات لممارسات أخرى سيُكشف أمرها في تسريبات قادمة لا محالة.

أنواع مهمام التجسس

1- تجسس هجومي: من أجل التجسس على العدو من خلال اختراق منظومة حواسيبه ومواقعه الإلكترونية ومهاجمة شبكات العدو بالفيروسات والتخريب وتدمير منظوماته الإلكترونية.

2- تجسس رقابي: من خلال مراقبة وسائل التواصل الاجتماعي ومراقبة حركة الأموال ومراقبة إيميلات وحواسيب المشتبه بهم وحتى مراقبة حركة عجلات الشرطة والجيش ضمن منظومة GPS.

3- تجسس وقائي: لصد تجسس العدو وتحصين شبكة حواسيب الدولة والأجهزة الأمنية لحماية الشبكات من الفيروسات وأي محاولات تخريبية ويتمثل ذلك بالتحول الرقمي.

آفاق التجسس الإلكتروني وفوائده

يتيح التجسس الإلكتروني إمكانية التنصت والتصوير من خلال اختراق حواسيب المستهدفين أو هواتفهم ومن ثم تشغيل اللاقطة والكاميرا للجهاز، دون أن يشعر المستهدف وسرقة معلومات وبيانات الجهاز المستهدف، لذا يلصق البعض شريطًا على كاميرا اللابتوب خوفًا من أن يفعّلها الهاكرز.

يتيح التجسس الإلكتروني اختراق البث التليفزيوني وبث ما يريده العدو، ولعل ما فعله الحوثيون في اليمن باختراق إحدى القنوات الحكومية السعودية وبث فيلم عن حقائق الحرب من هذه القناة واسعة الانتشار خير دليل على ذلك، بل إن أحد الهاكرز استطاع عام 2006 أن يخترق منظومة الطائرات الأمريكية بدون طيار وهو جالس في بيته بتقنيات لم تكلفه أكثر من 35 دولارًا.

التجسس الإلكتروني يتيح اختراق ملفات العدو والعبث بها وسرقتها وتهديده ومن ثم تجنيده، فعند سرقة وتهكير ملفات العدو وخوفه من كشف سره يتحول إلى مصدر يمكن بعدها تجنيده بسرية.

وكذلك يتيح التجسس الإلكتروني تنظيم وإدارة شبكات تجسس وهمية وتنظيم وإدارة شبكة اختراق

وتنظيم وإدارة شبكة استقراء وإحصاء واستبيان وتنظيم وإدارة شبكة للحرب النفسية والإشاعة وكشف الأهداف والخطط وتجنيد مقاتلين ونشر أخبار كاذبة.

تطبق أغلب الدول المتقدمة التجسس الإلكتروني على المواطنين والمشتبه بهم واستهداف هواتفهم وحواسيبهم وتضعهم تحت المراقبة التي تتباع مراسلاتهم ونشاطهم وجميع تحركاتهم.

رابط المقال: https://www.noonpost.com/36070/