انتهى زمن العملاء: هذه هي وسائل الاستخبارات الأمريكية في التجسس

كتبه أحمد عزيز | 22 أغسطس ,2016

منذ عقود طويلة وتحديدًا مع نهايات السبعينات، والجميع يعلم أن محكمة مراقبة الاستخبارات الخارجية للولايات المتحدة الأمريكية متساهلة للغاية، ولم ترفض طلبات التجسس التي يقدمها كل من مكتب التحقيقات الفيدرالي أو وكالة الأمن القومي، سواء للتجسس على الأفراد داخل أو خارج أراضيها أو على الدول.

ومؤخرًا أكدت وزارة العدل الأمريكية، أن المحكمة التي تحمل اسم FISC تم تأسيسها في عام 1978 للتعامل مع طلبات الجهات الحكومية بمراقبة والتجسس على الأجانب والمشتبه بهم، لم ترفض أي طلبات تجسس خلال عام 2015 بالكامل، ووافقت على طلبات التجسس التي وصل عددها إلى 1457، وهي خاصة بالمراقبة الإلكترونية الممنوحة لأغراض الاستخبارات الأجنبية، وتضم اعتراض الاتصالات، بما في ذلك البريد الإلكتروني والمكالمات الهاتفية والرسائل النصية، وهي معلومات تؤكد ما كشفت عنه تسريبات عميل وكالة الأمن القومى السابق إدوارد سنودن، في 2013، والتي تثبت تورط المحكمة في السماح بالتجسس بمساعدة شركات الإنترنت والاتصالات السلكية واللاسلكية.

ادعاءات وفضائح

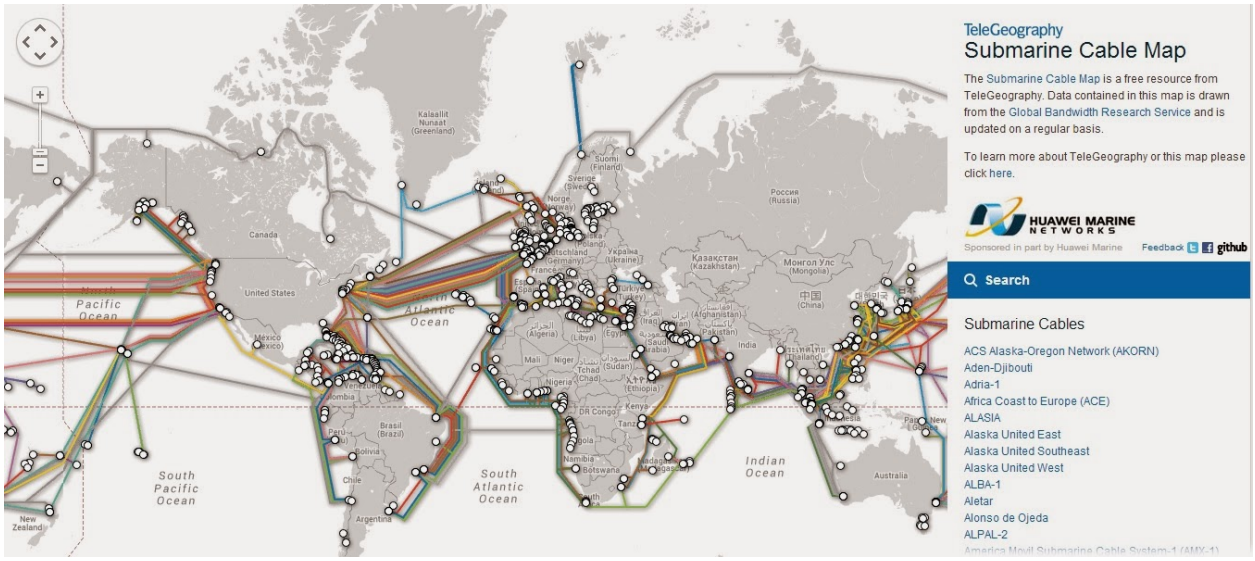
تقرير وزارة العدل الأمريكية يكشف زيف ادعاءات الولايات المتحدة المستمرة بحرصها على حماية خصوصية المواطنين الشخصية، ويؤكد تورطها في عمليات التجسس، والتي غالبًا ما تنفي قيامها بها، أو تبررها برغبتها في حماية أمنها القومي، وهي في ذلك تستخدم كل المتاح لها من أدوات تكنولوجية حديثة أولها الغواصات.

وتفيد المعلومات المتداولة بأن الولايات المتحدة لديها أسلوب متطور للغاية في ساحة المعركة الرقمية، فعلى سبيل المثال الجيش الأمريكي يستخدم غواصاته كمنصات للقرصنة تحت الماء، وتمثل تلك الغواصات عنصرًا هامًا من استراتيجية الإنترنت في أمريكا، فهي تعمل بصورة دفاعية لحماية نفسها والبلاد من الهجوم الرقمي، ولكن لديها دورًا آخر تؤديه في تنفيذ هجمات إلكترونية على عدد من البلدان الأخرى، طوعتها الحكومة للاستفادة من كابلات الاتصالات تحت البحر قبالة الساحل الروسي، وتسجيل الرسائل التي يتم ترحيلها ذهابًا وإيابًا بين القوات السوفيتية، وهذا الأمر دفع وكالة الأمن القومي لوضع كابلات الألياف تحت الماء، كجزء من جهازها لجمع المعلومات الاستخبارية على امتداد العالم.

جاسوس تحت الماء

يدعم تلك التصورات ما أفادت به تقارير عسكرية منشورة على أكثر من موقع، أهمها موقعي "بريكنج ديفينس" و"ذي إنترست" الأمريكيين، تؤكد أن الغواصات الأمريكية تأتي مجهزة مع الهوائيات المتطورة، التي يمكن استخدامها لاعتراض والتلاعب في حركة الاتصالات الخاصة بالدول الأخرى، خاصة على شبكات ضعيفة أو غير مشفرة.

التقارير أشارت إلى أن الغواصات النووية الأمريكية تعمل كمقار متحركة للتجسس على شبكات الإنترنت للدول الأخرى، حتى إن الغواصات المتقاعدة من العمليات الحربية أصبحت مقرات متنقلة لشن حربًا عبر شبكات الإنترنت ضد العديد من الدول من أعماق المحيطات.



كابلات الإنترنت

تاريخيًا بدأ التجسس عبر البحار بالكابلات التي مدتها الولايات المتحدة في الأعماق أثناء الحرب الباردة؛ للتجسس على روسيا لكن الأمر تطور مع ظهور وسائل الاتصال الحديثة مثل "الواي ـ فاي"، ويسعى حاليًا الأسطول الأمريكي لترقية برامج بعينها، لتحسين وزيادة مدى التنصت للغواصات.

سلاح الجو

لم تتوقف وسائل واشنطن للتجسس عند الغواصات، وطورتها خلال السنوات العشرين الأخيرة للطائرات بدون طيار، خصوصًا طائرة "جلوبال هوك"، والتي تعد واحدة من طائرات التجسس بدون طيار الأكثر تطورًا في الجيش الأمريكي، والتي يمكنها أن تتعقب شخصًا واحدًا على الأرض من ارتفاع 60 ألف قدم، ووفقًا لتصريح أحد المسؤولين بالجيش الأمريكي، فإن الطائرة تغطي العالم بصورة يومية طوال اليوم وعلى مدار الأسبوع، وهي بذلك توفر معلومات استخبارية كبيرة لكبار صناع القرار.

يرجع ظهورها بشكل أولي إلى ثلاثينات القرن الماضي، وكان أول استخدام عسكري لها في العام 1960، حين كاد يتفجر الوضع بين أمريكا والاتحاد السوفيتي، بسبب إسقاط الأخير طائرة تجسس أمريكية على الأراضي السوفيتية، وبعد تلك الفترة احتكر الجيش الأمريكي تكنولوجيا الطائرات بدون طيار طوال العقود الماضية، لكن بدأ الأمر يتغير في السنوات الأخيرة، قبل أن تسعى العديد من جيوش البلدان، مثل روسيا وباكستان وإيران والصين وجيوش أخرى إلى امتلاك هذه التكنولوجيا، بعدما كانت محتكرة من قبل للجيش الأمريكي وبريطانيا وإسرائيل.

وخلال السنوات الأخيرة دعم الجيش الأمريكي إمكانيات تصغير حجم الطائرات بدون طيار للقيام بعمليات أدق في التجسس والاغتيالات، وعمل فريق من الباحثين في جامعة جونز هوبكنز، بالتعاون مع مكتب البحث العلمي للقوات الجوية الأمريكية في قاعدة رايت باترسون الجوية في أرلينغتون بولاية فيرجينيا، على تطوير ما أسموها "مركبة جوية دقيقة" تتولى مهام مختلف أنواع التجسس، وهي مركبة قادرة على التسلل خلسة مع الرياح إلى "أماكن العدو"، والمناطق الحضرية المكتظة بالناس والمباني السكنية، بحيث يمكن السيطرة عليها من مسافة بعيدة، وهي مجهزة بكاميرا وميكروفون مدمج، ويمكنها كذلك اغتيال أفراد بعينهم بالهبوط على جلد الإنسان المستهدف، وغرس إبرتها المتناهية الصغر لحقنه بالسموم، أو أخذ عينات الحمض النووي الوراثي.

ولم تكتف الولايات المتحدة باستخدام هذه التقنية في التجسس بل تجاوزتها لاستخدامها في الحروب الخارجية خصوصًا حربي العراق وأفغانستان لتقليل حجم خسائرها البشرية من جنودها.

التجسس المنزلي

لم تتوقف محاولات الولايات المتحدة عند هذا الحد، وطورت وسائلها للتجسس على الأفراد والدول بقرصنة أجهزة الكمبيوتر، وكشفت شركة "كاسبرسكي" لبرامج الحماية، عن كيفية قيام وكالة الأمن القومي الأمريكية، بإدخال برامج تجسس خفية في الأقراص الصلبة التي تصنعها شركات مثل وسترن ديجيتال، وسيجيت وتوشيبا وغيرها، من الأقراص التي تم بيعها في بعض دول منطقة الشرق الأوسط، أبرزها إيران وروسيا وباكستان وأفغانستان والصين ومالي وسوريا واليمن والجزائر؛ للتجسس على أجهزة الكمبيوتر بها، وشملت أهدافها منشآت حكومية وعسكرية وشركات اتصالات وبنوكًا وشركات طاقة، وباحثين نوويين ووسائل إعلام ونشطاء إسلاميين.

برامج التجسس الأمريكية التي كشف عنها في السنوات الأخيرة تعد من أكبر البرامج، التي أثارت القلق والخوف في جميع أنحاء العالم دون استثناء، خصوصًا وأن تلك العمليات التجسسية قد شملت أقرب الحلفاء، الأمر الذي تسبب بحدوث أزمات أمنية ودبلوماسية، دفعت العديد من الحكومات والدول والشركات إلى اعتماد أساليب جديدة في حماية نفسها ومواطنيها من عمليات التجسس التي تقوم بها الحكومات وغيرها من عمليات سرقة البيانات.

شبكات المحمول

شبكات المحمول هي الأخرى لم تسلم من المحاولات الاستخباراتية الأمريكية، حيث كشف عدد من الوثائق المسربة من قبل إدوارد سنودن، أن وكالة الأمن القومى تجسست على مئات الشركات والمنظمات على المستوى الدولى، من خلال استغلال نقاط ضعف في تكنولوجيا الهواتف الخلوية، بما يمكن من استغلالها في الاختراق والمراقبة، ووضعت بعض الخطط لإدخال عيوب جديدة على أنظمة الاتصال تمكنها من اختراقها، ونجحت وكالة الأمن القومي في جمع معلومات تقنية عن حوالي 70%من شبكات الهواتف على مستوى العالم.

وتمكنت واشنطن عبر استخدام أجهزة "ديرت بوكس" التي تحاكي أبراج إرسال الهواتف النقالة، في كشف بيانات عن موقع المستخدم وهويته الخاصة، من خلال إطلاق إشارات مماثلة لتلك التي تنقلها أبراج الهاتف النقال التي تستخدمها شركات الاتصالات، وتلتقطها الهواتف بصورة عادية.

رابط المقال : https://www.noonpost.com/13549/