تحليلات وآراء

من الشيفرة المكتوبة الى البيانات الرقمية
تطور تقنيات جمع المعلومات الاستخبارية

بقلـــم
حســن فاضــل سليــم
باحث في مركز حمورابي للبحوث والدراسات الاستراتيجية

مركز حمورابي
للبحوث والدراسات الاستراتيجية

2026

تأسس مركز حمورابي للبحوث والدراسات الإستراتيجية عام 2008 بمدينة بابل (الحلة)، وحصل على شهادة التسجيل من دائرة المنظمات غير الحكومية المرقمة 1Z71874 بتاريخ 2012/12/25، بوصفه مركزا علميا بحثيا يهتم بدراسة الموضوعات السياسية والمجتمعية، فضلاً عن الاهتمام بالقضايا والظواهر الراهنة والمحتملة في الشأن المحلي والإقليمي والدولي، ويتعامل مع باحثين من مختلف التخصصات داخل العراق وخارجه، وتحتضن بغداد المقر الرئيسي للمركز.

للتواصل

العراق - بغداد - الكرادة

+964 7810234002

hcrsiraq@yahoo.com

www.hcrsiraq.net

مركز حمورابي للبحوث والدراسات الاستراتيجية

مقدمة

عكف البشر منذ الأزل خلال الحروب على ابتكار الادوات والطرق اللازمة لنقل المعلومات حول تحركات اعدائهم او ممارسة التظليل ضدهم، حيث اعتمدت عمليات التجسس تلك على طابع السرية التي تساهم في استمرار تدفق المعلومات الاستخبارية، ومن بين الأدوات التي ساعدت على حفظ هذه الأسرار، هي عملية التشفير للنصوص والرسائل المكتوبة والتي يمكن من خلالها نقل المعلومات برسالة مرمزة برموز يصعب على العدو فهمها عند اكتشافها، مما يسهل حفظ تلك المعلومات من التسريب، وقد تطورت اساليب التشفير والترميز وكسر الشيفرات عبر الزمن كما تطورت الرسائل المشفرة وادوات إرسالها وبثها، وصولاً إلى التطور التكنولوجي الذي زاد من كمية رصد وتدفق البيانات عبر الشبكات الرقمية، ما افرز مشكلة اضافية لا تتعلق بكيفية فك تشفير الرسائل التي يتم أعراضها فحسب بل مشكلة تتعلق بكيفية التعامل مع الكم الهائل من البيانات الواردة، وربطها وتحليلها واستخلاص دلالات ومعلومات استخبارية منها. تحاول هذه المقالة قراءة تطور استخبارات الإشارة من عمليات التشفير عبر الرسائل المكتوبة يدوياً وصولا لعصر الذكاء الاصطناعي والبيانات الضخمة.

أولاً: من الكتابة السرية الى التعمية وكسر الشيفرات

تشير المعطيات التاريخية الى ان الشعوب القديمة في حضارات وادى الرافدين ووادي النيل عرفوا التشفير في الرسائل، وذلك بهدف اخفاء محتوى الرسائل عن الآخرين من غير المصرح لهم بقراءتها، وقد استخدم اليونانيين والرومان التشفير في مراسلاتهم العسكرية لاسيما اسبارطة حيث كان الاسبارطيون يملكون ما يشبه جهاز تشفير الذي كان يتكون من عصا مدببة يلف حولها شريط من الجلد تكتب الرسالة عليه وعند فك الشريط من العصا تختلط الحروف وتضيع الكتابة، ولكن عند اعادة لف الشريط على عصا أخرى بنفس مقاسات العصا الأصلية تظهر الكتابة بوضوح، وكانت هذه الوسيلة تستخدم لنقل المراسلات بين القادة العسكريين أثناء الحروب.[1]

اما الرومان فقد ابتكروا ما عرف بشيفرة قيصر التي تقوم على استبدال كل حرف بالرسالة بما بعده بـ 3 حروف من الأبجدية على سبيل المثال استبدال حرف " أ " بالحرف "ث" حسب الأبجدية العربية ، وهو أسلوب اعتمده القائد الروماني (يوليوس قيصر) في مراسلاته العسكرية، حيث كان يستخدم هذا الأسلوب للتظليل والحفاظ على سرية المعلومات والمراسلات حتى أصبحت هذه الطريقة تعرف بـ(أبجدية يوليوس قيصر) .[2]

اما العرب فهم اول من حول طرق التشفير البدائية الى علم قائم بذاته عرف بـ(علم التعمية) وذلك باستخدام المعادلات الرياضية وقد كان للعالم (يعقوب بن اسحاق الكندي) الفضل في تحويل الشيفرة من نص يحتاج الى مفتاح لفهمه الى نص يمكن فك رموزه باستخدام طريقة تحليل التكرار التي ابتكرها، وأثبت من خلالها

---

[1] Gustavus J. Simmons, History of cryptology, Britannica, 11/8/2026, available at URL: https://www-britannica-com.translate.goog/topic/cryptology/History-Of-Cryptology

[2] دايفيد كان ، حرب الاستخبارات، ترجمة: عبد اللطيف افيوني، المؤسسة العربية للدراسات والنشر، بيروت ، 1987، ص17.

أن استخدام أسلوب الاحتمالات الرياضية عبر حساب التكرارات يمكنه فك النصوص المشفرة، وذلك عبر حساب الحروف المتكررة في النص، حيث لاحظ الكندي ان كل لغة فيها حروف متكررة بكثرة في الكلمات وحروف أخرى اقل استخداماً ، مثلا في العربية يتكرر حرفي (الالف واللام)، فمثلا لفك رسالة مشفرة يتم قراءتها ورصد الحروف الأكثر تكراراً فيها ومطابقتها مع نسب التكرار الطبيعية مع النص اللغوي الطبيعي حيث يتم ترتيب الحروف تنازليا من الأكثر الى الاقل تكرارا فيتم استبدال الحروف الأكثر تكرارا في النص المشفر بما يليها في جدول الترتيب التنازلي، وهكذا يتم كشف شيفرة من نوع شيفرة يوليوس قيصر دون الحاجة لمعرفة مفتاح النص المشفر.

وقد تطورت الشيفرة مع تطور عصر النهضة الاوروبية وتطور ادواتها حيث اصبحت الوسيلة الاساسية التي تكتب بها الرسائل الدبلوماسية والعسكرية، كما أصبحت الدول الأوروبية ونتيجة للحروب والصراعات فيما بينها تطور وتحدث شيفراتها باستمرار وتخصص أفراد لكسر شيفرات الاعداء والحلفاء على حد سواء لقراءة الرسائل ومعرفة نوايا واهداف الاخرين، ومع تطور وسائل الاتصال في القرن التاسع عشر برز نظام مورس مع اختراع التليغراف كوسيلة اساسية لبث الرسائل حول العالم، وهو نظام اكواد استخدم في عام 1844 يعمل بأسلوب (النقاط والشرطات) (. & -) حيث يتم تمثيل الحروف بواسطة النقاط والشرطات، وهو ما يسهل ارسال الرسائل عبر التليغراف المغناطيسي الذي كان يعمل بمبدأ النبضات الكهربائية حيث تمثل نبضة قصيرة الصوت نقطة (.) والنبضة الطويلة تمثل شرطة (-) وهي وسيلة باتت اساسية لنقل الرسائل المختلفة الدبلوماسية والعسكرية والمدنية، وقد تطلبت هذه البرقيات تشفيراً أيضا بواسطة أجهزة الاستخبارات فيما عملت أجهزة أخرى على محاولة فك تشفيرها.

وقد زادت الحروب من حدة التجسس والتجسس المضاد بين الدول ومعها ازدادت عمليات التشفير وفك التشفير تعقيداً، وقد خصصت أجهزة الاستخبارات الناشئة في الدول الغربية أقسام خاصة للتشفير وفك الشيفرات لرصد اعتراض وقراءة رسائل الاخرين.

وقد مثلت الحرب العالمية الأولى والحرب العالمية الثانية ذروة عمليات التشفير وفك التشفير، حيث ساهمت الشيفرات المكسورة بكشف خطط الجيوش المتحاربة لاعداءهم، كما حصل عندما كسر الامريكيين شيفرة البحرية اليابانية مما ساهم باستعداد البحرية الأمريكية لمعركة ميدواي البحرية الشهيرة التي انتصرت فيها الولايات المتحدة على البحرية اليابانية، واحيانا كان يتم استخدام الخداع والتظليل عبر ارسال رسائل بشيفرة العدو لتظليل جنوده بعد ان يتم كسرها بدون علمه.

وبفعل عمليات اعتراض رسائل وبرقيات التليغراف ظهرت الحاجة لظهور سلاح الاشارة في الاستخبارات العسكرية حتى بات يعرف هذا النوع باستخبارات الاشارة (SIGINT) (Signal Intelligence) والذي يعد اليوم فرعا مهما من فروع الاستخبارات.

ثانياً: ثورة الاتصالات والتشفير

أدى دخول شبكة البرق وجهاز التليغراف الى تطور منظومة استخبارات الإشارة ضمن الجيوش والبعثات الدبلوماسية المختلفة اذ برزت الحاجة الى تشفير الرسائل المرسلة عبر التليغراف وكذلك الى كسر تلك الرسائل، وقد أنشأت الولايات المتحدة ما يعرف بالغرفة السوداء المرتبطة بوزارة الخارجية حيث كانت تعمل على اعتراض رسائل البريد الخاصة بالبعثات الدبلوماسية وتعمل على كسر شيفراتها وقراءتها من اجل معرفة نوايا الخصوم والحلفاء وكنوع من أنواع الإنذار المبكر.

وقد زاد ظهور الراديو اللاسلكي الى زيادة الاتصالات الدبلوماسية والعسكرية وازدياد الحاجة الى تشفير الرسائل المرسلة عبر اللاسلكي، وقد اوجد ذلك معضلة الفضاء المفتوح حيث أصبحت الرسائل عبر اللاسلكي متاحة للجميع حيث يمكن اعتراضها بسهولة لكل من يملك هوائي لاقط.

وتعد من ابرز نجاحات استخبارات الإشارة ما قامت به استخبارات البحرية البريطانية عند تأسيسها لما عرف بالغرفة 40 التي اعترضت رسالة برقية عبر تليغراف البعثة الدبلوماسية الألمانية عرفت بـ(برقية زيمرمان) والتي تم فك تعميتها لمعرفة فحواها وقد اكتشفت الغرفة 40 انها كانت تمثل تحريضا من المانيا للمكسيك للدخول في الحرب ضد الولايات المتحدة وهو ما دفع الأخيرة لاتخاذ قرار المشاركة في الحرب العالمية الأولى ضد المانيا عام 1917.

وقد شكلت الحرب العالمية الثانية البواكير الأولى لانتقال عملية التشفير من الطرق اليدوية الى الالات الكهربائية ومن ثم الالكترونية في وقت لاحق، وذلك عبر اختراع عدد من تلك الالات التي استخدمت في الحرب.

ثالثاً: الماكنة والتعمية الرياضية

وفي الحرب العالمية الثانية برزت الة انجيما الألمانية التي كانت تقوم بتشفير الرسائل عبر اللاسلكي وتنظم الاتصالات التكتيكية بين القوات البرية والجوية والبحرية، اثناء العمليات العسكرية، حيث تولد الالة الالاف من الاحتمالات مما يعقد من عملية اختراقها. وقد نجح البولنديين قبل الحرب العالمية بـ7 سنوات من اكتشاف سر الالة وصنع الة مشابهة عرفت بـ(بومبا) سلموها الى الاستخبارات البريطانية قبيل اندلاع الحرب وغزو بولندا من قبل الالمان، عام 1939، كما فر خبراء الرياضيات البولنديين العاملين على الشيفرة الى بريطانيا وساهموا بدعم مشروع بليتشلي بارك البريطاني الذي اعتمد على خبراء الرياضيات في تفكيك الشيفرات الألمانية بعدما أنشأت الحكومة البريطانية مدرسة الشيفرة والتعمية الحكومية، والتي باتت تدرب خريجي الجامعات من اقسام الرياضيات على تفكيك الشيفرات الرياضية وساهمت مؤسسة بليتشلي بارك بتفكيك الشيفرات الألمانية خلال الحرب[1].

---

[1] دايفيد كان ، مصدر سبق ذكره، ص97- ص99.

وقد تمثل انجاز البريطانيين الأبرز في هذا المجال في تصميم اول حاسوب رقمي الكتروني عملاق استخدم حينها لكسر التشفير الألماني لاسيما كسر شيفرة جهاز سيمنس، الذي كان عالي التشفير وتستخدمه القيادة الألمانية العليا، لبث رسائلها بما فيها رسائل هتلر الى قادة الجبهات، وقد تم الاعتماد على الرياضيات الاحتمالية وحدها لتخمين الالة وطريقة عملها الفعلية وانشاء اول حاسوب رقمي عرف بحاسوب كلوكوس الذي ساهم بكسر الشيفرة وادى الى اكتشاف رسائل هتلر بما فيها وذلك خلال ساعات فقط[1].

وبفضل ذلك تمكن الحلفاء من قراءة خطط هتلر العسكرية بدقة. ومن أشهر النجاحات الاستخباراتية لهذه العملية هي معرفة تأكيدات القيادة الألمانية بأنهم ابتلعوا الطُعم إثر نجاح عملية التظليل التي قام بها الحلفاء، قبيل عملية إنزال النورماندي التاريخية (D-Day) مما ساهم بنجاح العملية واختصار عمر الحرب.

رابعاً: استخبارات الاتصالات والاشارة في الحرب الباردة

تطورت الاستخبارات بعد الحرب بما فيها استخبارات الإشارة بصورة عامة ودخل التصوير الجوي والتصوير بالاقمار الصناعية في عمليات الاستخبارات فظهرت أنواع جديدة من الاستخبارات مثل الاستخبارات التصويرية، وقد سرعت الحرب الباردة والصراع الاستخباري الذي اشتعل بين الاتحاد السوفيتي ودول المعسكر الغربي، في تسريع عمليات تطوير الاستخبارات المختلفة.

وقد أنشئ في الولايات المتحدة وكالة الاستخبارات المركزية CIA التي كانت تعمل على رصد المعلومات وتحليلها وتقديم تقديرات استخبارية لكن انشاء وكالة الامن القومي الامريكية ساهم بتغطية حاجة الولايات المتحدة من استخبارات الاتصالات والاشارة، حيث اصبحت هذه الوكالة مسؤولة عن تنظيم التنسيق الاستخباري ضمن تحالف العيون الخمسة وهو اشهر تحالف استخباري الذي يضم دول (بريطانيا، الولايات المتحدة الامريكية، كندا، استراليا، نيوزلندا) وكان هدف هذا التحالف تعزيز التعاون الاستخباري بين هذه الدول بمواجهة الاتحاد السوفيتي، وقد ساهم هذا التحالف بانشاء برنامج ايكيلون وهو اضخم برنامج سري عالمي لجمع البيانات والتنصت، تم تصميمه في أواخر ستينات القرن الماضي من قبل دول تحالف العيون الخمسة للتنصت على الاتصالات الدبلوماسية والعسكرية السوفيتية، وبعد الحرب الباردة توسع البرنامج ليشمل جمع واعتراض مختلف انواع الاتصالات حول العالم المدنية والعسكرية، ويعمل من خلال [2]:

1. الاعتراض الشامل: التقاط إشارات الأقمار الصناعية، والمكالمات الهاتفية، ورسائل البريد الإلكتروني، وحركة الإنترنت، والفاكس.

---

[1] المصدر نفسه.

[2] European Parliament, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), Rapporteur: Gerhard Schmid, Doc. No. A5-0264/2001 (Brussels, 2001).

2. **الفحص الآلي:** تمرير هذه البيانات عبر حواسيب عملاقة تبحث عن كلمات مفتاحية محددة (مثل: قنبلة، سلاح، اغتيال).

3. **التحليل الصوتي واللغوي:** القدرة على تمييز بصمات أصوات المتحدثين، وترجمة اللغات الأجنبية تلقائياً إلى الإنجليزية.

ولم تقتصر الاستخبارات في هذه المرحلة على اعتراض الاتصالات فحسب بل استخدمت صور الأقمار الصناعية والتصوير الجوي بكثرة حتى أصبحت المعلومات الاستخبارية لا تخبرنا بما يقوله الخصم فحسب بل أصبحت ترى أجهزة الاستخبارات ما يفعله الخصم ايضاً.

خامساً: من الإشارات والصور الى البيانات الرقمية

تميزت هذه المرحلة بثورة تكنولوجية ادت لتوسع الاتصالات الدولية من خلال تطور بنية التحتية للأنترنيت عبر شبكة كابلات الألياف الضوئية وظهور شبكة الويب، مما أدى لانتشار مواقع الانترنيت، وهو انتشار زاد من أهمية المصادر المفتوحة للحصول على البيانات الاستخبارية الخام، حتى ظهر ما يعرف باستخبارات المصادر المفتوحة (OSINT) (Open Source Intelligence) والتي ازدادت اهميتها بشكل كبير في جمع المعلومات الاستخبارية الرقمية، حيث باتت منصات التواصل الاجتماعي تمثل منجما من البيانات التي تعمل أجهزة الاستخبارات على استخراج البيانات منها كما أصبحت بعض أجهزة الاستخبارات تشتري بيانات المواقع الجغرافية وسجلات التصفح الشرعية من وسطاء البيانات (Data Brokers) دون الحاجة لطلب مذكرات تعقب رسمية.

وقد زاد تطور الحياة الذكية وظهور الهواتف الذكية والكاميرات المنزلية والأجهزة الذكية الاخرى في تعزيز عمليات الرصد ولاسيما استخبارات الإشارة فمع اختراع نظام الGPS وادخاله ضمن انظمة الهواتف الذكية المحمولة أصبحت هذه الهواتف ترسل إشارات تساعد في تعقب تحركات الافراد عبر الأقمار الصناعية، مما يساعد اجهزة الاستخبارات على رصد الافراد وتحركاتهم ومعرفة سجل مكالماتهم وحفظ بصمات الوجه والصوت وكذلك جمع البيانات حول حالتهم الصحية عبر تطبيقات الصحة والساعات الذكية، كل ذلك زاد من حجم البيانات التي باتت تصدرها هذه الوسائل التقنية الحديثة ما ادى الى مشكلة اكبر باتت تواجهها أجهزة الاستخبارات لا تتعلق بكيفية فك تشفير المحادثات والاتصالات بل بكيفية استيعاب هذا الكم الهائل من البيانات وتصنيفها وتخزينها، ما تتطلب منها بناء مراكز بيانات ضخمة تعمل على حفظ هذه البيانات إلكترونيا عبر فرزها وتصنيفها لاستخراجها وقت الحاجة بما يساعد أجهزة الاستخبارات على بناء ملفات تعريفية للالاف او الملايين من الافراد المراقبين حول العالم بالاضافة الى بيانات الأحداث والتطورات اليومية على المستويات كافة.

وبالتالي البيانات التي كان يتم سابقاً الحصول عليها من اعتراض اتصالات ورسائل العدو ومعرفة ما يقوله وكذلك من تصوير مواقعه ومعرفة ماذا يفعل، إلى الحصول على أدق المعلومات عليه من خلال القدرة على جمع المعلومات والتفاصيل الدقيقة عن أهله واصدقاءه عبر وسائل التواصل الاجتماعي، حيث باتت الاستخبارات اكثر قدرة عبر هذه الوسائل على جمع المعلومات حول الأشخاص بعدما كانت إمكانياتها التقنية سابقا تمكنها من جمع المعلومات عن الدول والجيوش والدبلوماسيين من خلال اعتراض الاتصالات او التنصت عليها.

سادساً: عصر البيانات الضخمة والذكاء الاصطناعي

مع ازدياد استخدام وسائل التواصل الاجتماعي وتنوعها الكبير ظهرت الحاجة بشكل اكبر لأتمتة عملية جمع وتحليل البيانات خاصة وان العناصر البشرية يمكن ان يستغرقون وقت طويل في تحليل البيانات المتاحة والتي لن يتمكنوا من استيعابها بالكامل مع تنوعها الكبير ومع اندلاع حروب وصراعات جديدة أصبحت فيها وسائل التواصل الاجتماعي جزء من المعركة الإعلامية والاستخبارية، وبدأ ثورة الذكاء الاصطناعي الذي بات يقلل من الزمن اللازم لتحليل البيانات ويساعد في استيعاب كم هائل منها وتصنيفها، بالتالي يمكن القول ان الاستخبارات في عصر الذكاء الاصطناعي باتت بحاجة اكبر لمراكز البيانات الضخمة التي ازدادت اهميتها في جمع وفرز البيانات وباتت مشكلة الاستخبارات حتى مع كل هذه الوسائل المساعدة هو استيعاب التطورات الهائلة والكم الهائل من التفاعل والسيولة حول العالم وتحليلها واستخراج المعلومات منها.

لكن دخول الذكاء الاصطناعي في ساحات المعارك ساهم بشكل كبير في تعزيز القدرات السيبرانية للجيوش حيث بات من خلال الذكاء الاصطناعي والتقنيات الحديثة استخدام الصور المنشورة على مواقع التواصل الاجتماعي وتحليلها لاستخراج المعلومات الاستخبارية وتحديد المواقع العسكرية والمدنية او المواقع الحيوية الاخرى، كما باتت أدوات الذكاء الاصطناعي مثل مشروع مافن تحلل الالاف من الصور والاتصالات الملتقطة والبصمات الصوتية للتعرف على الافراد وتسريع عمليات الاستهداف مما قلص الزمن اللازم لاتخاذ القرارات العسكرية الى الحد الأدنى وادى إلى استخراج بنوك اهداف حيوية يمكن ان يتم استهدافها.

لكن في عصر الذكاء الاصطناعي ومع تراجع دور البشر في الجمع والتحليل للاتصالات والاشارات وحتى بعض الصور يبقى هامش الخطأ موجودا نتيجة للبيانات التي يقوم البشر بتلقينها للذكاء الاصطناعي والتي يمكن ان يكون بعضها خاطئ ويؤدي لتصنيف الذكاء الاصطناعي لبعض الأهداف المدنية على أنها اهداف عسكرية.

كما أن استخدامه في عمليات الرصد واستهداف الافراد ادى لتوليده العديد من الأهداف المدنية التي ادت الى زيادة الخسائر في صفوف المدنيين.

أما بخصوص التشفير فقد طورت اجهزة الاستخبارات تشفير اكثر تعقيداً لا يعتمد على الرياضيات لوحدها باستخدام الذكاء الاصطناعي، ومن الأمثلة على ذلك استخدام التشفير العصبي الذاتي حيث تقوم أجهزة الاستخبارات باعطاء أوامر لنظامي ذكاء اصطناعي يمكن تسميتهما مثلا اليكس وبوب، مع وضع نظام ثالث معادي يسمى ايف للتنصت على المحادثة المشفرة ومحاولة كسر الشيفرة.[1]

والفائدة من هذه الطريقة هو تعزيز قدرة الذكاء الاصطناعي على توليد شيفرات معقدة بشكل تلقائي، يصعب حتى على بعض المبرمجين فهمها وتفكيكها.

اما الطريقة الثانية من التشفير فتعرف بالتشفير المتماثل بالكامل وذلك لمعالجة وتحليل البيانات المشفرة والمخزنة في السحابة الرقمية من خلال فك تشفيرها دون تعرضها للاختراق، حيث يقوم الذكاء الاصطناعي بمعالجة وتحليل البيانات وهي لا تزال داخل وضع التشفير التام، دون الحاجة لفكها. مما يمكن خوارزميات الذكاء الاصطناعي من فرز البيانات والبحث عن التهديدات دون الاطلاع على المحتوى الحقيقي إلا عند الضرورة القصوى[2].

بالمقابل تواجه الاستخبارات اليوم مع تطور الحواسيب الكمومية معضلة تشفير البيانات بشكل لا تستطيع تلك الحواسيب فائقة الدقة من فكها، حيث يمكن ان يؤدي انتشار هذه الحواسيب لتعزيز قدرة أجهزة الاستخبارات على التشفير والاخفاء او تعزيز القدرة على فكها واستخراج البيانات منها[3].

---

[1] Purushottam Singh, Sandip Dutta, and Prashant Pranav, "Optimizing GANs for Cryptography: The Role and Impact of Activation Functions in Neural Layers Assessing the Cryptographic Strength," Applied Sciences 14, no. 6 (2024): 2379, https://doi.org/10.3390/app14062379.

[2] Riccardo Magni, Carlo Tassi, and Emanuele D'Agostini, "Building Privacy-Preserving AI system: AI Inference on Encrypted Data with Fully Homomorphic Encryption," in 2025 International Conference (IEEE, 2025), https://ieeexplore.ieee.org/document/11165930.

[3] Cybersecurity and Infrastructure Security Agency (CISA), "Post-Quantum Cryptography Initiative," accessed August 16, 2026, https://www.cisa.gov/topics/risk-management/quantum.

وتستخدم الاستخبارات الذكاء الاصطناعي لاختبار وتوليد خوارزميات هندسية متعددة الأبعاد (تشفير قائم على الشبكية) ومحاكاة هجمات كمومية للتأكد من حصانة الأنظمة الخاصة بها[1].

كما أجهزة الاستخبارات بالاضافة الى التشفير تلجأ الى اخفاء البيانات وذلك من خلال قيام الذكاء الاصطناعي بدمج الشيفرات السرية داخل ملفات وسائط عادية (صورة، ملف صوتي، أو فيديو تكتيكي) بطريقة تبدو طبيعية تماماً لأي نظام مراقبة خارجي، وبمعدل تضليل وإفلات من الرصد يصل إلى أكثر من 98%، كما يقوم الذكاء الاصطناعي بتبديل الشيفرة ومفاتيحها بشكل تلقائي كلما استشعر وجود هجوم او محاولة اختراق دون تدخل البشر[2].

خاتمة

بناء على ما تقدم يمكن القول ان عمليات استخبارات الإشارة واعتراض المراسلات والاتصالات تطورت عبر الزمن من خلال تطور الحروب ووسائل جمع هذه المعلومات وتشفيرها، فقد كان البشر يجهدون انفسهم في عملية ابتكار ادوات تشفير وتعمية البيانات لاخفاءها عن الآخرين، وحماية سريتها، وقد ساهم تطور وسائل الاتصالات بتطور وسائل اخفاء هذه المعلومات من التشفير اليدوي مروراً باستخدام المكائن وصولاً الى استخدام الأجهزة الإلكترونية والحواسيب وانتهاءً بالذكاء الاصطناعي، وكل مرحلة من هذه المراحل كانت تزداد فيها صعوبة التشفير تعقيده، كما تظهر مشكلات جديدة في كيفية مواجهة وحماية الشيفرات، التي بات يتم توليدها تلقائياً بواسطة الذكاء الاصطناعي، بالإضافة إلى كل ماسبق تطورت الاستخبارات التصويرية استخبارات المصادر المفتوحة لتضيف طبقة إضافية من التعقيد في عملية جمع وتحليل البيانات حيث باتت الصور تعطي بيانات خام لاسيما عبر التصوير الجوي او عبر نشرها في وسائل التواصل التي تحولت لمناجم من البيانات المصورة المكتوبة.

هذه التطورات فرضت على الاستخبارات بناء مراكز بيانات عملاقة تدار بواسطة الذكاء الاصطناعي لاستيعاب الكم الهائل من البيانات وفرزها وتصنيفها وحتى المساعدة في تحليلها من اجل دعمعناصر التحليل الاستخباري بالتحديثات بصورة آنية وسريعة تسمح لهم مواكبة الأحداث والتطورات الدولية المتسارعة.

بالتالي يمكن القول ان جمع المعلومات الاستخبارية بالوسائل التقنية تطور بشكل هائل عبر الزمن وفقاً لمبدأ التحدي والاستجابة حيث فرضت تحديات الحروب الكبرى على الدول ايجاد وابتكار الوسائل المختلفة لحفظ سرية المعلومات وكشف المعلومات السرية عن خصومهم وذلك بهدف التقليل من عدم اليقين واكتساب ميزة استباقية إضافية على حساب الخصم سواء في وقت السلم ام الحرب.

---

[1] Ibid

[2] So-Yeon Yoon and Hyun Kwon, "Generative AI-Based Steganographic Techniques for Tactical Communication Message Concealment and Modification," in Information Security and Cryptology – ICISC 2025: 28th International Conference, Seoul, South Korea, November 19–21, 2025, Revised Selected Papers (Springer, 2025), 73–84, https://doi.org/10.1007/978-981-95-8034-7_4.