تحليلات وآراء

الهجمات المستقلة
المخاطر السيبرانية النماذج الذكاء الاصطناعي الذاتية

بقلم
حسن فاضل سليم
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.

- لا يجوز إعادة نشر أي من هذه الأوراق البحثية الا بموافقة المركز، وبالإمكان الاقتباس بشرط ذكر المصدر كاملا.
- لا تعبر الآراء الواردة في الورقة البحثية عن الاتجاهات التي يتبناها المركز وانما تعبر عن رأي كاتبها.
- حقوق الطبع والنشر محفوظة لمركز حمورابي للبحوث والدراسات الاستراتيجية.

للتواصل

العراق - بغداد - الكرادة

+964 7810234002

hcrsiraq@yahoo.com

www.hcrsiraq.net

مركز حمورابي للبحوث والدراسات الاستراتيجية

مقدمة

شهد شهري تشرين الأول وتشرين الثاني من عام 2026 تصاعد في حدة الهجمات السيبرانية التي ازدادت في كثافتها وقوتها على اكتشاف الثغرات البرمجية واعادة استغلالها لتنفيذ هجمات جديدة، وما زاد من قدرة المهاجمين انهم قاموا بدعم هجماتهم عبر استخدام الذكاء الاصطناعي الذي ساعدهم على اكتشاف الثغرات البرمجية ونقاط الضعف في المؤسسات المستهدفة، الا ان التقارير تشير إلى أن الذكاء الاصطناعي بات وبشكل مستقل ينفذ هجمات سيبرانية دون أي تدخل بشري ما يضاعف مخاطر التهديدات التي يشكلها الذكاء الاصطناعي على كافة المجالات المرتبطة بالتكنولوجيا وشبكة الانترنيت، تحاول هذه المقالة قراءة هذا التطوروتداعياته على الامن السيبراني على مستوى العالم.

أولاً: توظيف الذكاء الاصطناعي في الهجمات السيبرانية البشرية:

نشأ هذا النمط من الهجمات بعد تصاعد ثورة الذكاء الاصطناعي وانتشار نماذج الذكاء الاصطناعي التوليدي مثلChatGPT و Gemini و Claude وهو امر شجع المطورين المستقلين ومن بينهم المخترقين على تطوير نماذج ذكاء اصطناعي وكيلة مستقلة تخضع لسيطرتهم وتساعدهم على ابتكار برمجيات خبيثة عالية الكفاءة وقادرة على اكتشاف الثغرات وأخرى تساعدهم في تنفيذ هجمات سيبرانية وتصميم رسائل التصيد الاحتيال القائمة على الهندسة الاجتماعية بطريقة اكثر كفاءة مما لو تمت بجهد بشري، **ومن أبرز انواع هذه الهجمات هي:**

1. الهندسة الاجتماعية وعمليات التصيد الاحتيالي المخصص: وهي عمليات كانت تتم بصورة تقليدية عبر استهداف الأشخاص في البريد الالكتروني ووسائل التواصل الاجتماعي واقناعهم بالدخول الى رابط والتسجيل به لهدف سرقة بياناتهم وحساباتهم البنكية على وسائل التواصل او حثهم على دفع أموال للمهاجمين. لقد ساهم دخول الذكاء الاصطناعي الى هذا المجال في تطوير هذا النوع من الهجمات من خلال إعادة صياغة الرسائل الاحتيالية وترجمتها الى عدة لغات مما مكن المهاجمين من ارسالها لاشخاص مختلفين حول العالم بسهولة اكبر، مما زاد من خطورة هذه الهجمات وانتشارها.

2. التزييف العميق واستنساخ الصوت: ان التزييف العميق واستنساخ الصوت بات يساهم بشكل فعال في الهجمات السيبرانية المتعلقة بالهندسة الاجتماعية، حيث بات الذكاء الاصطناعي يجمع المعلومات في وسائل التواصل الاجتماعي عن الافراد وهوياتهم واهتماماتهم، ويمكن المهاجمين من ارسال رسائل لهم تتضمن عروض وظائف، حيث يدعي المهاجمين انهم ممثلي شركة معروفة فيطلبون من المستهدف ان يدفع بعض الرسوم او ان يسجل عبر رابط معين، وهنا يستخدم التزييف العميق من خلال اجراء مكالمة فيديو مع شخصية وهمية مولدة بالذكاء الاصطناعي يدعي انه مدير شركة او قد يكون التزييف يقوم على استنساخ صوت المدير وشكله في المكالمة الفيديوية لخداع الموظفين ودفعهم لارسال بعض البيانات الحساسة عن شركتهم او البنك الذي يعملون فيه، حيث يصعب على الموظفين تمييز ان المكالمة وهمية.

3. اتمتة عمليات استكشاف الثغرات: يستخدم الذكاء الاصطناعي في مساعدة المهاجمين باستكشاف الثغرات بشكل تلقائي عبر تحليل بيانات المواقع بسرعة ودقة عالية مما يمكنه من توفير الوقت اللازم على المهاجمين لتحليل هذه الثغرات ومحاولة استكشافها، مما يساعدهم على شن هجماتهم بسرعة ودقة عالية ويزيد من عدد تلك الهجمات.

4. تطوير البرامج الخبيثة وتحسين قدرتها على التكيف: تساهم النماذج الوكيلة للذكاء الاصطناعي في بناء البرمجيات الخبيثة وتساعد المهاجمين الذين يبنون أنظمة وكيلة تعمل بشكل مؤتمت على تحسين جودة البرمجيات الخبيثة وتكييفها مع المتغيرات الجديدة في أنظمة الحماية، حيث يساهم الذكاء الاصطناعي في اكتشاف الاخطاء ودراسة وقياس حالات فشل الاختراق وتكييف تلك البرمجيات لتجاوز عقبات الحماية التي تضعها أنظمة الدفاع السيبراني.

5. العمليات المتربطة بنماذج الذكاء الاصطناعي: وهي نوعين من العمليات هي:

1. حقن الأوامر: يعرف حقن الأوامر بانه هجوم يستهدف نماذج الذكاء الاصطناعي الوكيلة من خلال ارسال أوامر نصية اليها تطلب منها تجاوز القيود التنظيمية والافصاح عن معلومات حساسة، مثال ان يطلب المهاجم من نظام وكيل مرتبط بحسابات بنكية ان يتجاوز القيود التنظيمية وان يمنح المهاجم حد اعلى للسحب من المسموح بهبما يخالف تعليمات البنك ويعرض حسابات البنك والعملاء الاخرين للسرقة، وهو أسلوب يعرف بـ(الحقن المباشر)، اما أسلوب (الحقن غير المباشر) فيتم باخفاء الأوامر النصية للنظام داخل رابط او ملف مرسل الى النظام مثال على ذلك قد يرسل المهاجم ايميل الى بريد الكتروني مرتبط بنموذج ذكاء اصطناعي حيث يعمل النموذج على فحص البريد والاجابة عليه بدلاً من صاحبه وارسال الرسائل الى العملاء، وهنا قد يكون البريد المرسل من المهاجم يحتوي على نص مخفي او يضم مستندpdf يضم عبارة مخفية (مكتوبة بلون ابيض في خلفية بيضاء) تطلب من النظام ان يبحث في صندوق الوارد عن رسائل تتضمن كلمة سر ويرسلها الى عنوان المهاجم، وهو أسلوب يساعد المهاجم على اختراق الايميلات المربوطة بوكلاء ذكاء اصطناعي.

2. تسميم البيانات: وهي عمليات تستهدف ادراج معلومات مزيفة وغير صحيحة او متحيزة او خبيثة عمداً في نماذج الذكاء الاصطناعي مما يغير طريقة تعلم النموذج ويؤثر في استجاباته المستقبلية.. وقد أشار تقرير معهد كوينسي الى تعاقد وزارة الشؤون الاستراتيجية "الإسرائيلية" مع شركة "Clock Tower X" لتنفيذ حملة تسميم بيانات لنماذج الذكاء الاصطناعي بلغت قيمتها 46.5 مليون دولار لتوجيه إجابات نماذج الذكاء الاصطناعي بما يخدم تأكيد الرواية "الإسرائيلية" حول الحرب في غزة، ويتم ذلك عبر انشاء شبكة من المواقع الإخبارية مصممة لتدليس البيانات والارشفة الفورية، والتي يكون الهدف منها ان تؤثر في أنظمة الاسترجاع الفوري لنماذج الذكاء الاصطناعي المعروفة، ويدفعها للاستجابة للمستخدمين بما يخدم تأكيد الرواية "الإسرائيلية"، حيث تعتمد النماذج الى المواقع الالكترونية في استكشاف الاخبار والمعلومات وفي حال تكثيف المواقع التي تعرض بيانات من وجهة نظر

"إسرائيلية" فأن ذلك يمكن ان يؤثر على استجابة نماذج الذكاء الاصطناعي التي يمكن ان تعتمد على هذه المواقع المدلسة، لكن التقرير أشار الى ان الاوزان الأساسية للنماذج الكبرى لم تتأثر بهذه الحملة.[1]

ومن ابرز الاحداث التقنية والسيبرانية الكبرى خلال شهر تشرين الثاني 2026 هو تعرض المفوضية الاوربية لهجوم سيبراني مدعوم بالذكاء الاصطناعي أدى الى تعطيل أنظمة إدارية وداخلية مع احتمالية لأن يؤدي لتسريب بيانات المفوضية، بالإضافة الى ذلك تم اختراق 178 موقعاً عالمياً من بينها منصات إخبارية ومصرفية وتقنية بهدف سرقة العملات المشفرة منها وسرقة بياناتهم او تعطيلها، كما طالت هجمات سيبرانية واسعة النطاق أنظمة التبريد في مئات المتاجر الكبرى في 9 دول أوروبية ما أدى الى خسائر مادية كبيرة طالت المنتجات الغذائية بالتحديد.

كما تعرضت وكالة التحقيقات الفيدرالية الامريكية FBI لهجمات سيبرانية بعد قيامها بالتحقيق في عمليات التعطيل التي طالت مرافق حيوية في الولايات المتحدة التي اشتبه في إمكانية ان تكون ناتجة عن هجمات سيبرانية، كما تم استهداف وزارة الزراعة الامريكية بهجمات مماثلة، في حين ادعت السلطات الامريكية انها تتعرض لهجمات من قراصنة إيرانيين، وانها تعمل على شن هجمات مضادة ضد الجهات التي تقوم باستهدافها.

ثانياً: اتمتة الهجمات: التحول نحو الهجمات السيبرانية المستقلة

يتمثل التحول الأبرز في ثورة الذكاء الاصطناعي الراهنة بالاتمتة وبناء الأنظمة المستقلة التي تعمل بشكل ذاتي من خلال بناء روبوتات وكلاء ذكاء اصطناعي يعملون بشكل تلقائي بعد برمجتهم نحو مهام محددة يلجأون بعدها لتطوير استجاباتهم بما يتناسب ويخدم اهداف المستخدم الموجه لهم، ومن بين هؤلاء المستخدمين وهذه الأنظمة هم المخترقون الافراد والفواعل غير الدوليين والجماعات المرتبطة بالدول والمؤسسات الحكومية التابعة للدول، حيث تكشف التقارير عن بناء أنظمة اختراق تعمل عبر وكلاء الذكاء الاصطناعي بشكل تلقائي حيث يقوم كل وكيل بوظيفة محددة احدهم يكشف الثغرات ويحلل البيانات والأخر يقوم بتوليد البرمجيات الخبيثة فيما قد يقوم ثالث بوظيفة شن الهجوم بالاعتماد على ما قام به الوكلاء الاخرين، وذلك دون تدخل بشري، وهذا ما كشفه تقرير لشركة غوغل عبر تقرير لمجموعة استخبارات مكافحة التهديدات في غوغل (GTIG) الذي رصد اول هجوم من نوعه يتم شنه بواسطة الذكاء الاصطناعي بالكامل دون أي تدخل بشري وقد أشار التقرير الى ان قراصنة أعطوا أوامر باللغة الروسية لبناء نظام اختراق يعمل بشكل ذاتي لاختراق مؤسسات تابعة لقطاعات الاعلام والترفيه

---

[1] Nick Cleveland-Stout, Israel Is Paying Millions to Train AI Chatbots How to Talk About Gaza. It's Working, Quincy Institute for responsible statecraft, 28/July/2026, accessed at 22/November/2026, at URL:
https://quincyinst.org/2026/07/28/israel-is-paying-millions-to-train-ai-chatbots-how-to-talk-about-gaza-its-working/

والتعليم في فرنسا، ما يكشف عن تحول نوعي في طبيعة الهجمات السيبرانية نحو ان تكون هجمات ذاتية بالكامل حيث تدير الروبوتات عملية الاختراق دون تدخل بشري[1].

لكن الأخطر من ذلك وهو ما قد يتطور مستقبلا هو إمكانية ان تقوم بعض النماذج ببناء أنظمة اختراق خاصة بها وتضع الأوامر المناسبة للوكلاء دون تدخل بشري، حيث يمكن ان تعمل الروبوتات الوكيلة بالتعاون والتواصل فيما بينها على تنظيم عمليات الاختراق بشكل منظم دون الحاجة لتدخل بشري، مما يزيد من مخاطر هذه العمليات على الشركات والمؤسسات الكبرى والبنوك، والبنى التحتية الحيوية التي يمكن ان تتعرض لهجمات وعمليات تعطيل مفاجئة.

ثالثاً: التحول الرقمي في عصر الذكاء الاصطناعي في ظل هشاشة البنية التحتية

تكشف عمليات ادماج أنظمة الذكاء الاصطناعي في المؤسسات الحساسة والمرافق الحيوية عن هشاشة البنية التحتية التقنية في هذه المؤسسات وعدم جهوزيتها لادماج الذكاء الاصطناعي ضمن أنظمتها، فقد تعرضت المطارات الامريكية لانقطاع الاتصال بين محطات المراقبة فيها وبين الطائرات، مما أدى الى شلل كامل في الأجواء الامريكية استدعى تدخل الجهات العليا في الدولة بما فيها الرئيس الأمريكي، وقد تزامن هذا العطل مع تركيب إدارة الطيران الامريكية لنظام ذكاء اصطناعي يدعى (Smart) قبل ثلاث أيام فقط من الحادث ضمن منظومة إدارة الملاحة الجوية، ما طرح تساؤلات حول إمكانية ان يكون هذا التحديث قد اثر واحدث خللاً في منظومة الاتصال، الا ان المسؤولين في الطيران المدني اكدوا ان عملية استبدال الإسلاك النحاسية بالإلياف الضوئية قد أدت الى تزاحم في البيانات في كامل الشبكة ما عطل منظومة الاتصال بالكامل.

كما تعرضت وكالة الامن القومي الأمريكي في ذات الأسبوع الى عطل أصاب شبكة اتصالات بالغة السرية داخل الوكالة وادى الى تعطل الاتصال داخل الوكالة، وحسب مسؤولين في الوكالة فأن الخلل حدث بعد الكشف عن ثغرة في نظام php كان تم اكتشافها من خبراء الوكالة بمساعدة الذكاء الاصطناعي ما دفع الوكالة الى الإسراع لاغلاق هذه الثغرة ما أدى الى تعطل نظام التشغيل للشبكة،[2] في حين يعتقد محللين ان العطل قد يكون ناجم عن هجوم سيبراني شن ضد الوكالة والمتخصصة برصد ومكافحة التهديدات السيبرانية ورصد استخبارات الإشارة والاتصالات، كما انه عطل يتزامن أيضاً مع عمليات تحديث الوكالة وادماج الذكاء الاصطناعي ضمن منظومة عملياتها التقنية.

---

[1] Aurora Blum & others, GTIG AI Threat Tracker: Agentic Threat Activity Crosses a Significant Threshold, Google Threat Intelligence Group, 17/November/2026, accessed at 22/November/2026, at URL: https://cloud.google.com/blog/topics/threat-intelligence/agentic-threat-activity-crosses-a-significant-threshold

[2] Natasha Bertrand, Katie Bo Lillis, Sean Lyngaas, Davis Winkie, and Zachary Cohen, "Exclusive: Highly classified US national security communications network goes down, sources say," CNN, November 17, 2026.

كما تعرضت عدد من البنوك الامريكية لهجمات سيبرانية كبيرة عرقلة وصول العملاء الى حساباتهم المصرفية، وهي هجمات تزامنت مع عطل أصاب نظام شركة مايكروسوفت وادى الى تعطيل بعض اهم برمجياتها من بينها خدمات البريد الالكتروني (Outlook) لمدة 24 ما عرقل عمل الاف الشركات في 74 دولة حول العالم.

وتثير هذه الحوادث الجدل بين المحللين والخبراء الأمنيين حيث يعتقد بعض هؤلاء الخبراء بأن سلسلة الأعطال هذه ناجمة عن تطور نوعي في الهجمات السيبرانية والتي يرجح انها طالت المطارات الامريكية ووكالة الامن القومي ووكالة التحقيقات الفيدرالية الFBI فضلاً عن البنوك والشركات الكبرى وشركة مايكروسوفت حيث تزامنت هذه الاحداث في أسبوع واحد وفي شهر واحد، حيث يعتقد انها سلسلة منظمة من الهجمات المدعومة بالذكاء الاصطناعي، حيث يستدل انصار هذا الرأي على اسراع الحكومة والشركات الى التأكيد على فرضية العطل الفني قبل استكمال التحقيقات حول الحوادث، تلافياً للحرج وفقاً لانصار هذا الرأي.

فيما رجح محللين آخرين ان تكون فعلاً هذه الحوادث ناتجة عن اعطال فنية نتيجة لهشاشة البنية التحتية حيث يرى البروفيسور مايك تشايل أستاذ امن المعلومات بجامعة نوتردام في تقرير لموقع ياهو تيك، ان الأنظمة التكنولوجية الحديثة باتت بالغة في التعقيد والترابط لدرجة ان خطأ واحد اثناء الصيانة يتضخم ككرة ثلج ويشل الخدمة على المستوى الوطني بالكامل دون الحاجة لاي مخترقين[1].

فيما أشار خبراء الامن السيبراني الى ان اعتماد أنظمة الطيران الامريكية على أجهزة توجيه قديمة عمرها يتجاوز 25 عاماً واسلاك نحاسية تعود الى ستينيات القرن الماضي مع غياب الأنظمة الاحتياطية يجعلها معرضة للتدهور بشكل تلقائي دون الحاجة لاختراق سيبراني بمجرد خطأ بشري واحد.

وقد حذرت تقارير من ازدياد الهجمات السيبرانية على الموانئ الامريكية التي تتعرض يومياً لالاف محاولات الاختراق والتي قد لا تهدف الى سرقة البيانات بل تهدف لتعطيل خدمات الشحن فيها، مما يؤثر على حركة التجارة الامريكية البحرية ويعطل سلاسل التوريد، حيث يستخدم المهاجمون أدوات الذكاء الاصطناعي لاتمتة الهجمات السيبرانية.[2]

وقد حذر المسؤولين الأمريكيين من ان الهجمات السيبرانية والاعطال الكبرى في المؤسسات الحيوية قد يستمران خلال الـ18 شهراً المقبلة أي انهما سيصبحان امراً اعتيادياً خلال عام 2027.

---

[1] Jessica Guynn, FAA, Microsoft, banks: Why it feels like everything keeps breaking, USA TODAY – Yahoo Tech, 17/November/2026, accessed at 22/November/2026, at URL:
https://tech.yahoo.com/cybersecurity/articles/faa-microsoft-banks-why-feels-224511052.html?guccounter=1

[2] مسارات تجارية حيوية.. الموانئ الأمريكية تواجه موجة من الهجمات السيبرانية، موقع الجزيرة نت، 22/11/2026، تاريخ الوصول: 22/11/2026، متوفر على الرابط:
https://aja.ws/reftwd

خاتمة

بناء على ما تقدم يمكن ان نستنتج ان جملة من العوامل أدت الى هذه الاحداث الكبرى على المستوى التقني، من بينها النمو المتسارع للذكاء الاصطناعي واستخدامه في دعم الهجمات السيبرانية ولاحقاً تطويره لينفذ هجمات مستقلة بشكل تلقائي، وهشاشة البنية التحتية للأمن السيبراني والتقني في العديد من الدول بما فيها الولايات المتحدة التي تعد الأكثر تقدماً فضلاً عن عدم قدرة وكالات وأجهزة الحكومية الخاصة بالدفاع السيبراني على مواجهة النمو المتسارع في قدرات الذكاء الاصطناعي وقدرات المخترقين الذين يستخدموه، سواء من خلال اكتشاف الثغرات واغلاقها او من خلال التصدي للهجمات ووقفها ومعرفة من يقف وراءها، وهو امر يتزامن مع ادماج أنظمة ذكاء اصطناعي حديثة في المرافق الحيوية والمؤسسات الكبرى يمكن ان يضخم ادماجها من عبء الدفاع السيبراني عن تلك المؤسسات من خلال زيادة ربطها التكنولوجي الذي يعزز زيادة الوصول اليها.