The Effect of Artificial Intelligence on Cybersecurity[#]

Maha Allam[(1)*]

(1) Researcher The Egyptian Center for Thought and Strategic Studies

Abstract

Received: 1/2/2026

Accepted: 10/5/2026

Published: 23/7/2026

* ***Corresponding Author:***
-

DOI:
https://doi.org/10.59759/law.v5i2.1961

Artificial intelligence (AI) is one of the most important and rapidly evolving technologies, aiming to enhance the ability to develop applications and systems that mimic human mental capabilities. Therefore, it can be argued -according to a preliminary analysis- that innovation has the potential to enhance cybersecurity, and its manifestations in AI applications further enhance this capacity. Accordingly, AI can analyze massive amounts of data at extraordinary speed, automate security operations, predict potential threats, and even enable proactive measures. Conversely, AI poses an increasing number of risks and threats to cybersecurity as a result of its exploitation in numerous diverse technical systems across various fields, as well as within various forms of warfare tools, and as part of a wide range of weapons and military applications. Consequently, the dual impact of AI on cybersecurity has made the relationship more complex and multifaceted.

Key words: Artificial Intelligence - Cyberspace - Technology - Cybersecurity – Security.

□

[#] A special issue for the Third International Conference, entitled: **Artificial Intelligence, A Legal Vision Towards a Sustainable Future**.

تاثير مزدوج ..اثر الذكاء الاصطناعي على الامن السيبراني

مها علام [1]

(1) باحث، المركز المصري للفكر والدراسات الاستراتيجية.

ملخص

يعد الذكاء الاصطناعي واحدًا من أهم وأسرع التقنيات تطورًا، والذي يهدف إلى تعزيز القدرة على تطوير أنظمة تحاكي القدرات العقلية البشرية. لذا، يمكن القول – وفق تحليل أولي – إن الابتكار لديه القدرة على تعزيز الأمن السيبراني، وانعكاساته في تطبيقات الذكاء الاصطناعي تزيد من هذه القدرة. وذلك بالاستناد إلى قدرته على تحليل كميات هائلة من البيانات بسرعة خارقة، وأتمتة العمليات الأمنية، ناهيك عن التنبؤ بالتهديدات المحتملة بل وتمكين التدابير الاستباقية. وفي المقابل، يفرض الذكاء الاصطناعي على الأمن السيبراني عددًا متزايدًا من المخاطر والتهديدات كنتيجة لتوظيف هذه التقنيات في العديد من الأنظمة التقنية المتنوعة بالمجالات المختلفة، وكذلك ضمن أدوات الحرب بأشكالها المتفاوتة، وأيضًا كجزء من مجموعة واسعة من الأسلحة والتطبيقات العسكرية. ومن ثم، فإن التأثير المزدوج للذكاء الاصطناعي في الأمن السيبراني جعل العلاقة أكثر تعقيدًا وتحمل العديد من التشابكات.

الكلمات الدالة: الذكاء الاصطناعي– الفضاء السيبراني – التكنولوجيا – الأمن السيبراني – الأمن

المقدمة

شهد مفهوم الأمن مسارًا ممتدًا من التطور الذي جاء كاستجابة للتغيرات التي لحقت ببيئته المحلية والدولية. ومن ثم، فقد ساهم بزوغ الفضاء السيبراني وتغلغله في كافة مناحي الحياة في ظهور وبلورة الأمن السيبراني، والذي عرفه "رودني رويستر" بأنه "يهدف إلى حماية الأجهزة والشبكات والبرامج والبيانات من التهديدات السيبرانية الخارجية".[1] هذا، ويعد الذكاء الاصطناعي واحدًا من أهم وأسرع التقنيات تطورًا، والذي يهدف إلى تعزيز القدرة على تطوير أنظمة تحاكي القدرات العقلية البشرية (مثل: التعلم، واتخاذ القرارات، وحتى الإبداع).[2]

[1] Nicholas Patterson, **What is Cybersecurity and Why is It Important?**, Southern New Hampshire University, 30 October 2024, available at: https://www.snhu.edu/about-us/newsroom/stem/what-is-cyber-security, 15/02/2025.

[2] جيونغكي ليم، **الذكاء الاصطناعي التوليدي: ما هو، وما الميزات التي لا يتمتع بها، وما يمكن أن يمثله للأمم المتحدة**، الأمم المتحدة، 18 يوليو 2023، متاح على: https://www.un.org/ar/208258، 2025/02/13.

وفي هذا السياق، تواجه الدول وضعًا إشكاليًا كنتيجة للتأثير المزدوج الذي تحمله العلاقة بين الذكاء الاصطناعي والأمن السيبراني. إذ يتضح أن الفضاء السيبراني قد ساهم في ظهور "القوة السيبرانية" التي اعتبرها "جوزيف ناي" تعبر عن شكل جديد من أشكال القوة المرتبط بـ "امتلاك المعرفة التكنولوجية والقدرة على استخدامها". كما نظر إليها أيضًا بوصفها القدرة على استخدام الفضاء السيبراني لـ "خلق مزايا والتأثير في الأحداث في بيئات تشغيلية أخرى".[1] وهو التحليل الذي يمتد قياسًا إلى دعم وتعزيز الأمن السيبراني بالاستناد إلى القوة السيبرانية التي تحملها التقنيات الحديثة، وفي مقدمتها الذكاء الاصطناعي.

وعلى هذا النحو، يمكن القول بشكل عام ووفق تحليل أولي إن الابتكار لديه القدرة على تعزيز الأمن السيبراني، وانعكاساته في تطبيقات الذكاء الاصطناعي تزيد من هذه القدرة؛ فتقنيات الذكاء الاصطناعي الفائقة التي تسمح بتحليل كميات ضخمة من البيانات بسرعة خارقة تعكس تغييرًا جذريًا في جمع المعلومات واكتشاف التهديدات واتخاذ القرارات، بما يزيد من فرص مواجهة التهديدات وتأطير الاستجابة المناسبة. وفي سياق أشمل، يتضح أن تأثير الذكاء الاصطناعي يتجاوز مهمة تحليل البيانات إلى الوصول لأتمتة العمليات الأمنية، وتقليل فرص الخطأ البشري، وزيادة كفاءة عمليات المراقبة والدفاع، ناهيك عن قدرته على التنبؤ بالتهديدات المحتملة بل وتمكين التدابير الاستباقية التي تعزز الأمن السيبراني بشكل أكبر وأشمل وأوسع.[2]

وعلى النقيض من ذلك، فقد جادل الضابط بالجيش الأسترالي "بي كي سينج"[3] بأن الفضاء السيبراني برز كبعد جديد لمهاجمة الخصوم وإخضاعهم دون قتال، معتبرًا أنه أضحى ساحة مناسبة لتطبيق "نظرية حرب المناورة" التي تستهدف فقدان الخصم لتماسكه وتفتيت قدرته على المواجهة وليس بالضرورة قتله بصورة مباشرة. ومن ثم، يصعب إغفال المخاطر المتزايدة التي تواجه الأمن السيبراني كنتيجة لتقنيات الذكاء الاصطناعي؛ فحالة الارتباط الدائم بين التكنولوجيا

[1] Joseph S. Nye, **Cyber Power**, (Massachusetts: Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, 2010), p. 4.
[2] Ehtesham Shahid, **The implications of AI for regional security**, Arab News, 30 May 2024, available at: https://www.arabnews.com/node/2519841, 03/09/2024.
[3] P.K. Singh, **Maneuver Warfare in Cyberspace**, (USA: Marine Corps War College, Marine Corps University, Marine Corps Combat Development Command, Quantico, 1997), pp. 36-40.

والحرب تبلور تأكيد رئيس مؤداه أن الابتكارات والتقنيات سريعة التطور تجلب مخاطر متقاطعة. الأمر الذي يعني أن الانتشار الآخذ في الاتساع للذكاء الاصطناعي قد جعله متضمن في العديد من الأنظمة التقنية بالمجالات المختلفة، وكذلك ضمن أدوات الحرب بأشكالها المتفاوتة، وأيضًا كجزء من مجموعة واسعة من الأسلحة والتطبيقات العسكرية.[1]

لذا، يتضح أن العلاقة بين الذكاء الاصطناعي والأمن تحمل العديد من التشابكات، بل وربما تفرض معادلة جديدة في التعامل مع الأمن؛ إذ إن الاعتماد على الذكاء الاصطناعي في هندسة الأمن السيبراني قد ساهم في تغيير معادلة الدفاع والهجوم، فضلًا عن حسابات ومعادلات الردع. ما يؤشر على أن الأمن السيبراني بصدد مرحلة جديدة من إعادة التأطير والتشكيل لا تتعلق فقط بالأدوات والتطبيقات، وإنما تتعدى ذلك إلى الفاعلين والمستخدمين والتهديدات.[2] واستنادًا إلى ذلك، تدور إشكالية الدراسة حول بحث وتحليل **أثر الذكاء الاصطناعي في الأمن السيبراني، وتركيزًا على الفرص التي يحملها الذكاء الاصطناعي لدعم وتعزيز الأمن السيبراني، وكذا التهديدات والمخاطر التي يفرضها**. إذ أن التحديد الدقيق لخريطة الفرص والتهديدات سوف يساعد في تبني الاستراتيجية الأنسب التي من شأنها ليس فقط مواجهة المخاطر المحتملة والتهديدات القائمة، وإنما تعزيز الدولة لأمنها القومي بشكل عام.

[1] Ioana Puscas, **AI and International Security… Understanding the Risks and Paving the Path for Confidence Building Measures**, (Switzerland: UNIDIR, 2023), p. 7.

[2] محمد الكويتي، الأمن السيبراني في عصر الذكاء الاصطناعي، ترينذز للبحوث والاستشارات، **اتجاهات استراتيجية (25)**، (نوفمبر 2023)، ص9.

أولا: تطور المفهوم.. من الأمن إلى الأمن السيبراني:

تتعدد المعاني المرتبطة بالأمن طبقًا لتعدد الرؤى والاتجاهات والنظريات والاقتراحات؛ وقد تم النظر إليه في صورة أولية بوصفه يعني الإحساس بالطمأنينة التي يشعر بها الفرد سواء بسبب زوال المخاطر التي يمكن أن تهدد وجوده أو نتيجة لامتلاك الوسائل الكفيلة لدرئها.[1] لذا، يُعرف الأمن – في أبسط صور تعريفه – بأنه يتضمن "جميع التدابير التي يتم اتخاذها لتوفير الحماية"، كما يمكن النظر إليه بوصفه "التحرر من شعور القلق أو الخوف".[2] وفي سياق تطوري، التصقت بمفهوم الأمن أبعاد جديدة مع ظهور الدولة؛ إذ أمست – أي الدولة – تسعى من خلاله إلى الحفاظ على كيان الأمة وضمان استقلالها وحمايتها من أي قوى خارجية.[3]

هذا، وقد شهدت فترة ما بعد الحرب الباردة وبداية الحديث عن العولمة بروز منظومة مفاهيمية جديدة كانعكاس للتحولات الكبرى التي شهدتها البيئة الأمنية، وهو ما صاحبه بروز جدل حول مفهوم الأمن انصب – بشكل محوري – على تعميق وتوسيع مفهوم الأمن من حيث وحدة التحليل التي امتدت لتشمل الأفراد والجماعات والنظم الإقليمية، وكذا من حيث المضمون الذي اتسع ليشمل قضايا الاقتصاد والبيئة والمجتمع.. وغيرها.[4]

وهو الأمر الذي ساهم، وفق عدد من التحليلات، في تبلور شكلين للأمن: أحدهما سلبي والآخر إيجابي؛ ارتبط الأمن السلبي – إلى حد بعيد– بالأمن في صورته التقليدية التي تستند إلى القضايا الأمنية التي تكون الدولة أساسها والجيش أداتها. في حين اتصل الأمن الإيجابي بعلاج

---

[1] عطا محمد حسن صالح، **نظرية الأمن القومي في التقاليد الإسرائيلية**، (مصر: رسالة دكتوراه، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، 1981)، ص6.

[2] "**Security**", Collins Dictionary, available at: https://www.collinsdictionary.com/dictionary/english/security, 11/09/2024.

[3] عطا محمد حسن صالح، **مرجع سابق**، ص 13.

[4] خديجة عرفة محمد أمين، **مفهوم الأمن الإنساني وتطبيقاته في شرق آسيا**، (مصر: رسالة ماجستير، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، فبراير 2006) ص ص 31-38.

الثغرات التي لا يعالجها الأمن السلبي بالاستناد إلى تحليل أكثر عمقًا يتعلق بالجهات الفاعلة، والوسائل غير التقليدية لتعزيز الأمن، وكذا القيم الكامنة خلف الممارسات الأمنية.[1]

ومع بروز دور الفضاء السيبراني وتسارع وتيرة التطورات التقنية والتكنولوجية، اتخذ الأمن طابعًا وبعدًا سيبرانيًا بطريقة جعلته أصبح ركيزة أساسية في تعامل الدول مع الفضاء السيبراني. ويعد أول من استخدم مفهوم الأمن السيبراني كان علماء الحواسيب في بداية التسعينات لوصف جملة من المخاطر المرتبطة بالحواسيب والشبكات. وقد عرفته وكالة الدفاع السيبراني الأمريكية بأنه "فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام الإجرامي وضمان السرية والنزاهة وتوافر المعلومات".[2] ومن جهته، عرفه "رودني رويستر"، المحاضر في الأمن السيبراني بجامعة جنوب نيو هامبشاير، بأنه "يهدف إلى حماية الأجهزة والشبكات والبرامج والبيانات من التهديدات السيبرانية الخارجية، باستخدام الممارسات والأدوات التي يمكن أن تخفف أو تقلل من تأثير هذه التهديدات".[3]

وعلى هذا النحو، يتضح أن الأمن السيبراني يمثل مشكلة معقدة تتسم بعدم اليقين، إضافة إلى كونه ديناميكي يتطور بصورة هائلة، الأمر الذي يصعب من اللحاق المستمر بالأخطار؛ إذ أن التداخل بين العالم الفيزيائي والفضاء السيبراني قد خلق تهديدات جديدة لسيادة الدول وأمنها القومي.[4] ومن ثم، تجادل بعض التحليلات بوجود **استراتيجيتين للأمن السيبراني:**

- **استراتيجية ضيقة:** تركز – بشكل أساسي – على الأمن السيبراني في بعده المادي، والتي تشمل حماية البنية التحتية، وكشف عمليات التسلل، وتبني استراتيجية الاستجابة السريعة لحرب المعلومات، والتنسيق المخابراتي بين القطاعين العام والخاص.

---

[1] "**الأمن في العلاقات الدولية: بين التنظير والواقع الدولي**"، مجلة العلاقات الدولية، 20 سبتمبر 2023، متاح على: https://irajournal.academy/2023/08/26/security-theory-reality/، 2025/01/11.

[2] "**What is Cybersecurity**?" America's Cyber Defense Agency, 1 February 2021, available at: https://www.cisa.gov/news-events/news/what-cybersecurity , 12/08/2023.

[3] Nicholas Patterson, **op. cit**.

[4] Paul Cornish, Rex Hughes & David Livingstone, **Cyberspace and the National Security of the United Kingdom: Threats and Responses**, (UK: Chatham House Report, March 2009).

- **استراتيجية واسعة:** تتمحور حول تجاوز التحركات السابق ذكرها إلى التركيز على القوة الناعمة في الفضاء السيبراني، والتي تعتمد على تأطير المنظومات الخاصة بالأخلاق والأعراف والقيم. وتستند كذلك إلى تعزيز الاتصالات وإتاحة المعلومات للجميع، مع تعميق التنسيق بين الحكومة ومنظمات المجتمع المدني.[1]

ثانيًا: المقصود بالذكاء الاصطناعي وأنواعه:

تُرجع بعض التحليلات الإرهاصات الأولى للذكاء الاصطناعي إلى فترة الحرب العالمية الثانية على خلفية تطوير آلات الكمبيوتر التناظرية المصممة للتحكم بشكل أكثر فاعلية وكفاءة في بعض الأسلحة. ففي عام 1943، قدم "وارن ماكولوتش" و"وولتر بيتس" نموذجهما للخلايا العصبية الاصطناعية، التي تُعتبر أول نموذج للذكاء الاصطناعي، على الرغم من أن المصطلح لم يكن موجودًا. ولاحقًا، اقترح العالم البريطاني "آلان تورينج"، في عام 1950، تجربة عُرفت فيما بعد باسم "اختبار تورينج"، تهدف لتحديد ما إذا كان بإمكان الآلة أن تمتلك سلوكًا ذكيًا مشابهًا للإنسان. [2]

وبشكل عام، شهدت فترة الخمسينيات وأوائل الستينيات بعض الجهود المبذولة لإنتاج (آلات تفكر)، وفي مقدمتها ظهور "السلاحف الإلكترونية"، التي ابتكرها العالم البريطاني "دبليو جراي والتر". ومن ثم، فقد حظيت الأجيال الأولى من القنابل الذكية وأنظمة التسلح الأخرى الموجهة بالردود الاسترجاعية باهتمامٍ واسعٍ، كما غذت هذه الأجهزة السيبرناتيكية الرغبات المتعلقة بتوطيد الروابط بين الإنسان والآلة. وهو الأمر الذي ساهم في تنامي المساعي المتعلقة بعمليات اتصالات وقيادة وتحكم غير محدودة جغرافيًا وبلا نهاية[3].

---

[1] Thomas E. Copeland, The **Information Revolution and National Security**, (USA: Strategic Studies Institute, Army war College, Pennsylvania, August 2000), p.121.

[2] "**History of artificial intelligence**", Iberdrola Group, available at: https://www.iberdrola.com/innovation/history-artificial-intelligence#:~:text=However%2C%20it%20was%20not%20until,term%20did%20not%20yet%20exist, 02/02/2025.

[3] Joan Broadhurst Dixon & Eric J. Cassidy (Editors), **Virtual Futures: Cyberotics**, (New York: Technology and Posthuman Pragmatism, Routledge, 1998), p. 34.

وعلى هذا النحو، فقد طرح العالم الأمريكي "جون ماكارثي" مصطلح الذكاء الاصطناعي – للمرة الأولى – في خطاب ألقاه بالمؤتمر الدولي الثاني عن الآلات الذكية في عام 1955، معتبره كفرع من علم الحواسيب يركز على إنشاء آلات ذكية بإمكانها أداء المهام التي تتطلب الذكاء البشري.[1] واتصالًا بذلك، قاد "مكارثي" تطوير أول لغة برمجة للذكاء الاصطناعي، لغة "ليسب LISP"، خلال فترة الستينيات.[2] وفي حين اتجهت جامعة ستانفورد إلى تبني تعريف "ماكارثي" بشأن الذكاء الاصطناعي، إلا أنها ذهبت إلى أبعد من ذلك، معتبرة أن الآلات أمست قادرة على التعلم، على الأقل إلى حد ما يماثل البشر.[3]

وفي هذا السياق، فقد عرفته الولايات المتحدة في القانون الوطني للذكاء الاصطناعي لعام 2020 بأنه "نظام آلي قادر، ضمن مجموعة مُحددة من الأهداف التي يُحددها الإنسان، على تقديم تنبؤات أو توصيات أو اتخاذ قرارات تُؤثر على بيئات حقيقية أو افتراضية".[4] بينما عرفه قانون الاتحاد الأوروبي الخاص بالذكاء الاصطناعي على أنه "نظامًا قائمًا على الآلة مصممًا للعمل بمستويات مختلفة من الاستقلالية، وقد يُظهر القدرة على التكيف بعد النشر، والذي يستنتج،

---

[1] أحمد عنتر، **الذكاء الاصطناعي.. أبهى صور التفاعل بين البشر والتكنولوجيا**، الجزيرة، 24 ديسمبر 2023، متاح على:
https://www.ajnet.me/tech/2023/12/24/%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D8%A3%D8%A8%D9%87%D9%89-%D8%B5%D9%88%D8%B1-%D8%A7%D9%84%D8%AA%D9%81%D8%A7%D8%B9%D9%84-%D8%A8%D9%8A%D9%86.2024/09/04 ،

[2] "History of artificial intelligence", **op. cit**.

[3] "**Artificial Intelligence Definitions**", Stanford University, September 2020, available at: https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf, 03/09/2024.

[4] "**Artificial Intelligence (AI)**", US Department of State, available at: https://www.state.gov/artificial-intelligence/, 05/03/2025.

بالنسبة للأهداف الصريحة أو الضمنية، من المدخلات التي يتلقاها، كيفية إنشاء مخرجات، مثل: القرارات أو التوصيات أو التنبؤات، يمكنها أن تؤثر على البيئات المادية أو الافتراضية".[1]

ومن جهته، قدم معهد ستوكهولم الدولي لأبحاث السلام SIPRI تقسيمًا لتكنولوجيا الذكاء الاصطناعي قائمًا على ثلاث طبقات؛ تعد الأولى هي طبقة الأجهزة الأساسية لتطوير أنظمة الذكاء الاصطناعي (مثل: أجهزة الاستشعار، وشرائح الكمبيوتر)، بينما تتضمن الثانية برمجة الذكاء الاصطناعي المتعلقة بتصميم تقنيات الذكاء الاصطناعي قبل أن تنتقل لمرحلة التطبيقات.[2] وقد حددت مجموعة الخبراء رفيعة المستوى التابعة للاتحاد الأوروبي (AI HLEG) المجالات المتعلقة بهذه الطبقة، وهي:

- **الاستدلال:** المرتبط ببرمجة سلوك نظام الذكاء الاصطناعي ضمنًا أو صراحةً.
- **التعلم:** المتعلق بتقنيات وأساليب التعلم الآلي التي تسمح لأنظمة الذكاء الاصطناعي بـ "تعلم كيفية حل المشكلات التي لا يمكن تحديدها بدقة، أو لا يمكن وصف طرق حلها بقواعد الاستدلال الرمزي".
- **الذكاء الاصطناعي المتجسد (الروبوتات):** وثيق الصلة بعمل أنظمة الذكاء الاصطناعي في العالم المادي.[3]

أما الطبقة الثالثة فهي التطبيقات، التي تمثل التجسيد الملموس والاستخدام النهائي لأنظمة الذكاء الاصطناعي، ويغلب تقسيمها لفئتين عامتين؛ تتصل الأولى بالقطاعات، كالتعليم والصحة.. وغيرها، بينما تتعلق الثانية بنوع المهمة أو مضمون التطبيق، مثل: حل المشكلات وإدارة البيانات..إلخ.

---

[1] "**EU Artificial Intelligence Act**", Article 3: Definitions, available at: https://artificialintelligenceact.eu/article/3/, 17/01/2025.

[2] Vincent Boulanin, Kolja Brockmann & Luke Richards, **Responsible Artificial Intelligence Research and Innovation for International Peace and Security**, (Sweden: Stockholm International Peace Research Institute (SIPRI), Stockholm, November 2020), p. 2.

[3] **Ibid.**

وفي هذا السياق، يجري تقسيم الذكاء الاصطناعي إلى ثلاثة أنواع وفقًا لقوته، أي قدرته على محاكاة الخصائص البشرية، والتكنولوجيا التي يستخدمها للقيام بذلك، وكذا تطبيقاتها في العالم الحقيقي، وهي:[1]

1- **الذكاء الاصطناعي الضيق:** الذي يتمتع بنطاق ضيق من القدرات، ويحاكي السلوك البشري وليس الذكاء البشري، وتتم برمجته للقيام بوظائف معينة داخل بيئة محددة.

2- **الذكاء الاصطناعي العام:** الذي يتساوى مع القدرات البشرية، ولديه القدرة على تمييز العواطف والاحتياجات والمعتقدات والعمليات الفكرية للكائنات الذكية الأخرى، ما يعكس قدرته على جمع المعلومات وتحليلها عبر تراكم المواقف.

3- **الذكاء الاصطناعي الفائق:** الذي يتمتع بقدرات أكبر من الإنسان، إذ لا يفهم المشاعر والتجارب البشرية فحسب، بل يتفاعل مع المشاعر والاحتياجات والمعتقدات والرغبات الخاصة به، ويعتبر نموذجًا لنظرية العقل (Theory of Mind) التي تمثل الجيل القادم من الآلات فائقة الذكاء.

ثالثا: الفرص التي يحملها الذكاء الاصطناعي لدعم الأمن السيبراني:

يمكن القول بشكل عام إن الاعتماد على "القوة السيبرانية"[2] سوف يزيد القدرة على تعزيز الأمن، وانعكاساتها في تطبيقات الذكاء الاصطناعي يضاعف من هذه القدرة، نظرًا لقدرة الذكاء الاصطناعي الاستثنائية على تحليل كميات هائلة من البيانات، وأتمتة العمليات الأمنية، والتنبؤ بالتهديدات المحتملة وتمكين التدابير الاستباقية.[3] الأمر الذي يعني أن تقنيات وأنظمة الذكاء الاصطناعي قد أصبحت بمثابة جنود الخط الأمامي الجدد بالاستناد إلى قدرتها على تحديد

---

[1] Eban Escott, **What are the 3 types of AI? A guide to narrow, general, and super artificial intelligence**, Codbots, 24 October 2017, available at: https://codebots.com/artificial-intelligence/the-3-types-of-ai-is-the-third-even-possible, 13/03/2025.

See Also

محمد الكويتي، **مرجع سابق**.

[2] Joseph S. Nye, **op. cit**.

[3] Ehtesham Shahid, **op. cit**

التهديدات والاستجابة لها في الوقت الفعلي، وغالبًا حتى قبل ملاحظة البشر لهذه التهديدات، فضلًا عن التنبؤ بالثغرات والهجمات السيبرانية المحتملة، بل وربما الاستعداد للقيام بضربات استباقية.[1]

لذا، يستخدم الذكاء الاصطناعي ثلاث آليات أساسية لمعالجة مشاكل الأمن المعقدة[2]:

- **تحليل الأنماط Pattern Insights**: يتميز الذكاء الاصطناعي بقدرته على التعرف على أنماط البيانات وتصنيفها، وحتى التي يصعب على البشر تحليلها، ثم يعرض هذه الأنماط على مسؤولي وفرق الأمن السيبراني لمزيد من الفحص والتحليل.
- **توصيات عملية Actionable Recommendations**: بناءً على الأنماط المحددة، تُقدم نظم وتقنيات الذكاء الاصطناعي توصيات عملية لمتخصصي وفرق الأمن السيبراني حول التدابير المناسبة.
- **التخفيف الذاتي Autonomous Mitigation**: يمكن لتقنيات وبرامج الذكاء الاصطناعي اتخاذ إجراءات مباشرة نيابةً عن متخصصي الأمن لمعالجة مشاكل الأمن.

وعليه، تنعكس الفرص التي يحملها الذكاء الاصطناعي لدعم وتعزيز الأمن السيبراني في عدد من الأمور:[3]

1- **توسيع نطاق الأتمتة**: تساهم تقنيات الذكاء الاصطناعي في تقليل الاعتماد على العنصر البشري في سياسات وبرامج وأنظمة الأمن السيبراني بما يساعد على تخفيض الأخطاء البشرية.[4]

2- **تصنيف الإنذارات الأمنية**: نظرًا للحجم المتزايد من الإشعارات والإنذارات الأمنية، سيما في المؤسسات الضخمة والحيوية، توفر تقنيات الذكاء الاصطناعي لمسؤولي وعناصر الأمن السيبراني تصنيفًا وفقًا لأولويتها ودرجة خطورتها.[1]

---

[1] **Ibid.**

[2] "**What is AI in cybersecurity**?", EC-Council University, available at: https://www.eccu.edu/blog/the-role-of-ai-in-cyber-security/, 13/03/2025.

[3] Michael C. Horowitz, Gregory C. Allen, Edoardo Saravalle, Anthony Cho, Kara Frederick and Paul Scharre, **Artificial Intelligence and International Security**, Center for a New American Security, July 2018, available at: https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security, 21/08/2024.

[4] **Ibid.**

3- **اكتشاف الثغرات السيبرانية:** جرى العمل على تطوير تقنيات تستخدم الشبكات العصبية والشبكات التنافسية التوليدية في اكتشاف الثغرات الأمنية. ويسمح نهج التعلم الآلي بالاستفادة من الخبرة السابقة من أجل التنبؤ بالثغرات والنقاط الأكثر ضعفًا وانكشافًا.[2]

4- **رسم خريطة التهديدات:** تساعد تقنيات الذكاء الاصطناعي في صياغة مصفوفة التهديدات مع تقدير درجة خطورة كل تهديد، بما يساهم في تخصيص الموارد بصورة أكثر كفاءة.[3]

5- **الفرق الحمراء الآلية:** تستغل العديد من الهجمات السيبرانية الثغرات الأمنية التي فشل مصممو الأنظمة في معالجتها أو تأمينها. لذا، يمكن استخدام تقنيات الذكاء الاصطناعي لتطوير أنظمة جديدة للتحقق بإمكانها اختبار البرامج تلقائيًا بحثًا عن الثغرات الأمنية السيبرانية قبل نشر وتشغيل البرامج الجديدة.[4]

6- **الأمن المعلوماتي:** يمكن أن يؤدي استخدام الذكاء الاصطناعي إلى تخفيف آثار التضليل داخل أنظمة المعلومات المتطورة؛ إذ يساعد فهم اللغة الطبيعية وأشكال أخرى من التعلم الآلي تدريب النماذج الحاسوبية على اكتشاف وتصفية محتوى الدعاية المزيفة والمضللة.[5]

7- **تعزيز سرعة الاستجابة للتهديدات السيبرانية:** لا تُعضد تقنيات الذكاء الاصطناعي من القدرة على كشف التهديدات فحسب، بل تعمل أيضًا على تقليل وقت الاستجابة لوقت قد يصل إلى بضع دقائق، ناهيك عما توفره – أي التقنيات – من تقارير مبسطة لفرق الأمن السيبراني من شأنها تسهيل عملية المعالجة واتخاذ القرار المناسب.[6]

[1] محمد الكويتي، **مرجع سابق**، ص50.

[2] Michael C. Horowitz & Others, **op. cit**.

[3] محمد الكويتي، **مرجع سابق**، ص52.

[4] Michael C. Horowitz & Others, **op. cit**.

[5] **Ibid.**

[6] "**The Promising Impact of AI in Software Security**", Intrusion, 03 May 2023, available at: https://www.intrusion.com/blog/the-promising-impact-of-ai-in-software-security/, 19/03/2025.

8- **تطوير تقنيات التمويه:** تعزز تقنيات وأنظمة الذكاء الاصطناعي من أدوات الخداع والتمويه التي تهدف إلى بناء جزء معزول من الشبكة كـ (نظام مزيف) بغرض خداع القراصنة أو الخصوم بحصولهم على معلومات تبدو حقيقية لصرف نظرهم عن النظام الحقيقي.[1]

واستنادًا إلى ذلك، يتضح أن التوسع في الاعتماد على نُظم وتقنيات الذكاء الاصطناعي يقدم لمسؤولي وفرق الأمن السيبراني "ذكاء محسن enhanced intelligence" يمكنها من دعم وتعزيز الأمن السيبراني، ولا سيما في مجالاته الرئيسة:[2]

- **تحديد وحصر الأصول:** إجراء جرد شامل ودقيق لجميع المستخدمين والأجهزة والتطبيقات التي يتم استخدامها، مع تصنيف وتقييم دورها وأهميتها.
- **تعيين احتمالات التعرض للتهديدات:** مواكبة التهديدات على اختلاف مستوياتها، وتمكين المؤسسات من تحديد أولويات التدابير الأمنية بناءً على احتمالية وقوعها وتأثيرها المحتمل.
- **تقييم فعالية الضوابط:** تقييم فاعلية وتأثير الأدوات والعمليات الأمنية الحالية لتعزيز الوضع الأمني.
- **التنبؤ بمخاطر الاختراق:** الكشف عن الثغرات الأمنية والتنبؤ بالاختراقات المحتملة من خلال دراسة المجالات الثلاثة سالفة الذكر، بما يُمكّن من تخصيص الموارد بشكل استباقي للتخفيف من آثارها.
- **الاستجابة للحوادث:** توفير رؤى سياقية لتحديد أولويات التنبيهات الأمنية والاستجابة الفورية لها، مع تحديد الأسباب الجذرية، وتحسين عمليات إدارة الحوادث.
- **تقديم الحلول الشفافة:** يساعد الذكاء الاصطناعي على توفير توصيات وتحليلات واضحة وشفافة، بالتوازي مع تعزيز التعاون والدعم من أصحاب المصلحة في المستويات المختلفة، بما في ذلك المستخدمون النهائيون، ومسؤولو الأمن، والإدارة.

رابعًا: المخاطر التي يفرضها الذكاء الاصطناعي على الأمن السيبراني:

على الرغم من الفرص الكبيرة التي يحملها الذكاء الاصطناعي لدعم وتعزيز الأمن السيبراني، فإنه يصعب إغفال وجود جملة من المخاطر والتهديدات، لا تتوقف عند الحدود التقنية

[1] محمد الكويتي، **مرجع سابق**، ص55.

[2] "What is AI in cybersecurity?", **op. cit**.

الضيقة وإنما تتجاوز ذلك إلى المجالات الأوسع التي تضر بل وربما تنال من الأمن القومي للدول. وهو ما جادل به "سينج"[1] حينما اعتبر الفضاء السيبراني ميدان جديد لمهاجمة الخصوم وإخضاعهم دون قتال ما يسمح بتوظيف "نظرية حرب المناورة".

وفي هذا السياق، فقد بلور كل من السياسي الأمريكي المحنك "هنري كيسنجر"، و"إريك شميت"، الرئيس التنفيذي السابق لشركة "جوجل"، و"دانيال هوتنلوشر" من معهد ماساتشوستس للتكنولوجيا، في كتابهم المشترك (عصر الذكاء الاصطناعي: ومستقبلنا البشري) مخاطر الذكاء الاصطناعي، وعلى رأسها تزايد فرص الوصول لمستقبل محتمل لم تعد فيه القرارات المحورية التي تحدد مصير العالم في يد البشر بشكل حصري.[2] كما اعتبر الكتاب أن حالة الدمج المتسارعة للذكاء الاصطناعي في الحياة اليومية تحمل انعكاسات هائلة، بما فيها سيولة الحدود الوطنية، ووجود فجوة بين مصالح الشبكات والدول.[3]

ومن ثم، يُواجه الأمن السيبراني تحديات وعقبات متزايدة كنتيجة لتطور تقنيات ونظم الذكاء الاصطناعي، وفي مقدمتها:[4]

- **اتساع نطاقات الهجمات القائمة والمحتملة:** يمثل اتجاه الدول لتوسيع اعتمادها على الرقمنة والتكنولوجيا بشكل عام، والتقنيات المتقدمة والفائقة على وجه الخصوص، زيادة نقاط الضعف والثغرات الأمنية.
- **تعدد جبهات الهجوم:** تظهر التهديدات السيبرانية عبر سُبل مُختلفة، مما يعقد من تحقيق الأمن السيبراني الذي يتطلب تأمين كافة نقاط الدخول الموجودة والثغرات المحتملة.
- **الإغراق بالبيانات:** يتجاوز حجم البيانات قدرة المُعالجة البشرية، مما استلزم دفع الدول للاعتماد أنظمة مُدعمة بالذكاء الاصطناعي، ما فرض بعدًا آليًا في عملية اتخاذ القرار.
- **ندرة مُتخصصي الأمن السيبراني:** يتطلب التطور الضخم والمتسارع لنظم وتقنيات الذكاء الاصطناعي تقدم مماثل في قدرات المسؤولين والقائمين على الأمن السيبراني.

---

[1] P.K. Singh, **op. cit**.

[2] Henry A. Kissinger, Eric Schmidt & Daniel Huttenlocher, **the Age of AI and Our Human Future,** (USA: Little Brown and Company, New York, 2021).

[3] **Ibid.**

[4] "What is AI in cybersecurity?", **op. cit**.

وفيما يلي تفكيكًا أكثر تفصيلًا لأبرز المخاطر والتهديدات التي يفرضها الذكاء الاصطناعي على الأمن السيبراني على النحو التالي:

1. تطوير الهجمات السيبرانية:

وفر الفضاء السيبراني فرصًا كبيرة أمام شن هجمات سيبرانية بإمكانها ليس فقط تجاوز بعدي الزمان والمكان، وإنما أيضًا تعزيز القدرة على إخفاء هوية القائم بها، وذلك بالاعتماد على ترسانة من الأسلحة الرقمية والسيبرانية ذات التكلفة المنخفضة كثيرًا مقارنة بترسانة الأسلحة التقليدية.[1] ومن ثم، توفر تقنيات الذكاء الاصطناعي إمكانيات أضخم لتطوير الهجمات السيبرانية من حيث حجم ونطاق العمليات وسرعة تحقيق اهدافها والتنوع في أدوات تنفيذها.[2] وتتميز الهجمات السيبرانية المدعومة بالذكاء الاصطناعي بخمس خصائص رئيسة (أتمتة الهجوم، كفاءة جمع البيانات، التصنيف والتخصيص، التعلم المعزز، استهداف الأفراد عالية الأهمية).[3]

2. الحروب الذكية والمعقدة:

على الرغم من الدور الذي لعبه الفضاء السيبراني في التطوير السريع للحروب السيبرانية بأشكالها المختلفة، فإن توسع انتشار نظم وتقنيات الذكاء الاصطناعي قد ساهم في استحداث حروب ذكية أكثر تعقيدًا تميل لأن تكون أكثر فتكًا وعنفًا وأشد قسوة، ولا تعتمد بالضرورة على العسكريين. ويرتبط بهذا الأمر، التأثير العميق لهذه التقنيات على دور البشر في الصراعات المسلحة؛ فالاعتماد المتزايد على أنظمة الأسلحة المستقلة القاتلة، كالطائرات بدون طيار، قد يتطور إلى منظومات أسلحة ذات قدرات فائقة في العمل المستقل.[4] ما يعني تزايد الاحتمالات

---

[1] مها علام، **الفضاء السيبراني وسيادة الدولة في العلاقات الدولية.. دراسة نظرية بالتطبيق على حالة الولايات المتحدة الأمريكية**، (مصر: كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، 2024)، ص ص 146-147.

[2] محمد الكويتي، **مرجع سابق**.

[3] Lucia Stanham, **Ai-Powered Cyberattacks**, CrowdStrike, 16 January 2025, available at: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/,14/02/2025.

[4] "**Looking into the future: Artificial intelligence and its impact on peace and security in Africa**", Amani Africa Media and Research Services, 12 June 2024, available at: https://amaniafrica-et.org/looking-into-the-future-artificial-intelligence-and-its-impact-on-peace-and-security-in-africa/, 12/09/2024.

المرتبطة بقدرة أنظمة الأسلحة المستقلة على تسريع وتيرة الحرب بطرق تتجاوز قدرة التدخل البشري، ما يجعل إنهاء الحرب أكثر إشكالية.[1]

3. زيادة مخاطر الإرهاب السيبراني:

عرف مكتب مكافحة الإرهاب التابع للأمم المتحدة الإرهاب السيبراني بوصفه يقوم على إساءة استخدام تكنولوجيا الاتصالات والمعلومات والتقنيات الرقمية الجديدة من قبل الإرهابيين "لارتكاب أعمال إرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها".[2] وعليه، يتضح أن الإرهابيين بات بإمكانهم استخدام أساليب جديدة للهجمات المادية باستخدام الطائرات المُسيرة أو السيارات ذاتية القيادة، وكذا تطوير الهجمات السيبرانية ضد البنى التحتية الحيوية، وأيضًا تمكين انتشار خطاب الكراهية والتحريض على العنف بشكل أسرع وأكثر فعالية، ناهيك عن إنشاء محتوى بلغات متعددة بطريقة تسهل من عملية التجنيد.[3]

4. توسيع نطاق الجرائم السيبرانية:

منذ بزوغ الفضاء السيبراني سعت العصابات ومجموعات الجريمة المنظمة لتوظيفه في أنشتطهم الإجرامية. وعليه، ظهر مفهوم "الكارتلات السيبرانية" cyber-cartels التي تستفيد بشكل استراتيجي من التقنيات الحديثة لتحقيق الربح وضمان الأمان وتوسيع التأثير عبر ثلاثة مجالات رئيسة؛ وهي: الجرائم السيبرانية، وأسواق الويب المظلمة، والعملات المشفرة.[4] واتصالًا بذلك، فقد ساعدت التقنيات المتقدمة هذه الكيانات على التوصل إلى المعلومات المهمة كـ (سجلات الاعتقال)، وتسهيل تزوير الأوراق الرسمية كـ (جوازات السفر)، والاعتماد على تقنيات المحاكاة

---

[1] Ioana Puscas, **op. cit**., p. 46.

[2] مكتب مكافحة الإرهاب التابع للأمم المتحدة، **أمن الفضاء الإلكتروني**، متاح على: https://www.un.org/counterterrorism/ar/cybersecurity، 05/03/2025.

[3] Vladimir Voronkov, A**lgorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes**, United Nations Interregional Crime and Justice Research Institute (UNICRI), available at: https://unicri.org/News/Algorithms-Terrorism-UNICRI-UNOCCT, 18/03/2025.

[4] Amanda Suárez, **Why Mexican Cyber-Cartels Threaten U.S. National Security**, Geopolitical Moniter, 24 June 2021, available at: https://www.geopoliticalmonitor.com/why-mexican-cyber-cartels-threaten-u-s-national-security/, 22/02/2022.

لاختبار العمليات قبل تنفيذها.[1] علاوة على ذلك، تعتمد "عصابات الجرائم السيبرانية" cybercrime gangs على الذكاء الاصطناعي التوليدي لإنشاء رسائل تصيد احتيالي بلغات متعددة، وروبوتات دردشة تتلاعب بالضحايا، ونشر معلومات مضللة على وسائل التواصل الاجتماعي بكثافة كبيرة. وقد أوضح مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن التهديد الأبرز هو التزييف العميق، وقد تتبع خلال الفترة من فبراير إلى يونيو 2024، زيادة بنسبة 600% في عدد مرات ذكر "التزييف العميق" في قنوات "تليجرام" الخاصة بمجرمي الإنترنت والمنتديات السرية.[2]

5. تراجع دور الدولة لصالح شركات التكنولوجيا العملاقة:

على الرغم من محورية دور الدولة في تحديد (قواعد اللعبة) سواء داخليًا بشكل "حصري" أو خارجيًا من خلال التعاون مع نظرائها، فإن التطوير المتسارع في تقنيات الذكاء الاصطناعي قد حمل مؤشرات على دور مؤثر للغاية لشركات التكنولوجيا العملاقة، بطريقة قد تؤثر بشكل واضح على أمن الدول بل وعلى دور الدولة.[3] واستنادًا لذلك، يتضح أن قدرة هذه الشركات على تحمل

---

[1] John T. Picarelli & Phil Williams, Information Technologies and Transnational Organized Crime.:In David S.Alberts and Daniel S. Papp (Eds.), **Information Age Anthology: National Security Implications of the Information Age,** (Washington DC: Library of Congress Cataloging-in-Publication Data, Volume II, August 2000), pp. 377-396)

[2] Nate Nelson, **Ai-Powered-Cybercrime-Cartels-Asia**, Dark Readings, 10 October 2024, available at: https://www.darkreading.com/threat-intelligence/ai-powered-cybercrime-cartels-asia, 22/03/2025.

[3] إيمان الشامخ، **الحكومات في مواجهة أباطرة التقنية.. هل انتهى زمان الدول وبدأ عصر حكم الشركات؟**، الجزيرة، 18 ديسمبر 2021، متاح على:
https://www.ajnet.me/midan/miscellaneous/2021/12/18/%D8%A7%D9%84%D8%AD%D9%83%D9%88%D9%85%D8%A7%D8%AA-%D9%81%D9%8A-%D9%85%D9%88%D8%A7%D8%AC%D9%87%D8%A9-%D8%A3%D8%A8%D8%A7%D8%B7%D8%B1%D8%A9-%D8%A7%D9%84%D8%AA%D9%82%D9%86%D9%8A%D8%A9-%D9%87%D9%84 ، .2024/01/21

مليارات الدولارات من الاستثمارات في التقنيات الفائقة ومنها الذكاء الاصطناعي يعني أنه بات بإمكانها أن تصبح "كيانات سيادية جديدة" تنافس وربما تنازع سلطة الدولة.[1]

6- استهداف ترابط المجتمعات:

تتميز وسائل التواصل الاجتماعي بانخفاض حواجز الدخول لها، مما يسمح للجهات الفاعلة المجهولة – الآلية في بعض الأحيان – بنشر محتوى مضلل أو كاذب أو عنصري للغاية، وهو المشهد الذي يتفاقم كنتيجة لقدرة بعض أنظمة الذكاء الاصطناعي على تضخيم هذا المحتوى على نطاق واسع.[2] وكذا، فقد أدى استخدام تقنيات الذكاء الاصطناعي لتلبية التفضيلات الفردية عبر توفير "أقنعة رقمية" إلى تعزيز تأثير ما يمكن وصفه بـ "غرف الصدى"، والتي تجعل المستخدمين الذين ظلوا في مساحة معلومات متجانسة لفترة طويلة أكثر عرضة للتماهي مع الأفكار المتأصلة وربما جنون العظمة، ما يعني تحفيز "الاستقطاب الجماعي".[3] وأيضًا توفر تقنيات الذكاء الاصطناعي إمكانية أتمتة automation التصيد الاحتيالي ما يزيد من فعالية هجمات الهندسة الاجتماعية، وهي المسألة التي تغذيها قدرة أنظمة الذكاء الاصطناعي على إنشاء عمليات تزوير واقعية ومنخفضة التكلفة للصوت والفيديو.[4]

7- ضرب تماسك الجبهة الداخلية:

يوفر الذكاء الاصطناعي فرص متزايدة لتوليد مقاطع مزيفة لنشر معلومات مضللة تؤدي لزعزعة استقرار الأنظمة السياسية.[5] ما يعني تزايد احتمالات توظيف هذه التقنيات في تنفيذ ما يُعرف بـ "العمليات المغطاة" التي تسعى – ضمن أبرز أهدافها – إلى تحريض المواطنين ضد حكوماتهم، وإثارة النزاعات السياسية والحروب الأهلية.[6] علاوة على ذلك، تتزايد الإمكانات المتاحة

---

[1] Gu, Hongfei. Data, Big Tech, and the New Concept of Sovereignty, **Journal of Chinese Political Science**, Volume 29, (May 2023).

[2] Michael C. Horowitz & Others, **op. cit**.

[3] Masaya Ohagi, **Polarization of Autonomous Generative AI Agents under Echo Chambers**, (Japan: Association for Computational Linguistics, Tokyo, 2024).

[4] Michael C. Horowitz & Others, **op. cit**.

[5] Vincent Boulanin, Kolja Brockmann & Luke Richards, **op. cit**., p. 6.

[6] مها علام، **مرجع سابق**.

للتمرد ضد الدولة، والذي يُوصف بـ "النشاط الاختراقي" Hacktivism، الذي يهدف إلى توظيف الرقمنة والتقنيات التكنولوجية المتطورة والإنترنت لتحقيق أهداف سياسية. ومن بين أشهر أنماطه:[1]

- تجمعات الاختراق Hacking collectives: التي تناضل لضمان الحرية على الإنترنت وعرقلة أي محاولة لتقييد الوصول إلى الشبكة أو إلى المعلومات.
- المحتلون السيبرانيون Cyberoccupiers: الذين يقومون بتدشين المدونات أو المنتديات أو صفحات مواقع التواصل الاجتماعي في سبيل دعم بعض القيم والأفكار، وانتقاد القيم والآراء السياسية السائدة.
- محاربو الإنترنت Cyberwarriors: الذين يقومون باستخدام تقنيات القرصنة في مهاجمة مؤسسات الدولة وكيانات إدارة الحكم لتحقيق مطالب سياسية أو اجتماعية.

الخاتمة:

بالاستناد إلى التحليل السابق، وفي ضوء التأثير المزدوج للذكاء الاصطناعي في الأمن بشكل عام، والأمن السيبراني على وجه الخصوص، يتضح أن العلاقة بين الذكاء الاصطناعي والأمن باتت أكثر تعقيدًا وتحمل العديد من التشابكات، بل وربما تفرض معادلة جديدة في التعامل مع الأمن والتحركات التي من شأنها تعزيزه. إذ إن الاعتماد على نُظم وتقنيات الذكاء الاصطناعي في هندسة الأمن السيبراني قد ساهمت في تغيير معادلة الدفاع والهجوم، ناهيك عن حسابات ومعادلات الردع. ما يؤشر على أن الأمن السيبراني بصدد مرحلة جديدة من إعادة التأطير لا تتعلق فقط بالأدوات والتطبيقات، وإنما تتعدى ذلك إلى الفواعل والتهديدات.[2]

وعلى الرغم من الفرص الكبيرة التي يحملها الذكاء الاصطناعي لدعم وتعزيز الأمن السيبراني، فإن المخاوف بشأن الذكاء الاصطناعي تتزايد بوتيرة متسارعة نظرًا لأن الاعتماد المتزايد للبشر على نظم وتقنيات الذكاء الاصطناعي في أنشطتهم اليومية واتجاه تطبيقات الذكاء الاصطناعي للسيطرة ستفرض تحديًا للحكم البشري المستقل؛ وهو ما يمكن أن يؤدي إلى خطر

[1] Dorota Żuchowska - Skiba, **Hacktivism**, December 2023, available at: https://www.researchgate.net/publication/377163085_Hacktivism, 15/02/2025.

[2] محمد الكويتي، **مرجع سابق**.

الانقلاب من قبل هذه الآلات ذاتية التعلم ضد الحكم البشري. وهو ما وصفه "ريموند كرزويل" بـ "لحظة التفرد" التي تصبح فيها الآلة في قوة وذكاء يماثل أو يزيد عن البشر، بما سيؤدي إلى إشكاليات حقيقية، تكون لها تبعات سياسية وأخلاقية وفلسفية معقدة.[1]

علاوة على ذلك، فإن تزايد حجم المخاطر والتهديدات التي يفرضها الذكاء الاصطناعي على أمن الدول ربما يؤدي إلى تراجع النمط التقليدي للدولة مقابل تعزيز نمط "الدول الافتراضية" التي عرفها "كيفن كولمان" بأنها "مجتمع غامض من الأفراد الذين يتعرفون على أنفسهم ويتشاركون في بعض الأمور الاجتماعية أو السياسية، أو المعتقدات والعقائد، أو الأفكار والقيم".[2] وقد اعتبرها عالم المستقبليات "توماس فراي" بأنها "دول بلا أرض ولا حدود"، مشيرًا إلى أن "إرادة" الجمهور هي التي ستحدد "مدى قابلية استمرار الدولة الافتراضية".[3]

وتبدو الإشكالية الأكثر إثارة للانتباه بشأن تهديدات ومخاطر الذكاء الاصطناعي تلك المتعلقة بتضخيم "الفجوة الرقمية" بين الدول أو الكيانات التي تملك قدرات أكبر على الابتكار في الذكاء الاصطناعي، وتلك التي تمتلك قدرات محدودة أو لا تمتلك قدرات لتطوير وابتكار تقنيات الذكاء الاصطناعي. وهو الأمر الذي يمكن أن يفضي عند لحظة ما إلى إعادة تأطير لأشكال جديدة من الاستعمار والتبعية قائمة على التصنيف التقني للدول.[4] ويرتبط بهذه المسألة تبلور مصطلح "الاستعمار الرقمي" Digital colonialism، والذي يعني "تركز التكنولوجيات والتقنيات

[1] Ray Kurzweil, **The Singularity Is Near: When Humans Transcend Biology**, (USA: The Viking Press, New York City, 2005).

[2] Kevin Coleman, **Virtual States in Cyberspace increase in size and number**, 15 November 2012, available at: https://defensesystems.com/articles/2012/11/15/digital-conflict-virtual-states.aspx , 5/8/2020.

[3] Thomas Frey, **The Virtual Country**, Futurist Speaker, 5 February 2009, available at: https://futuristspeaker.com/future-scenarios/the-virtual-country/, 20/03/2025.

[4] Yang Xiaoguang & Chen Kaihua, **Artificial Intelligence Risks and Governance from a National Security Perspective,** People's Forum Network - Chinese, 16 July 2024, available at: http://www.rmlt.com.cn/2024/0716/707544.shtml, 19/09/2024.

الناشئة والبنية التحتية والموارد اللازمة لنشرها بسرعة وبقوة عبر الأسواق في أيدي عدد قليل من الشركات".[1]

وعلى هذا النحو، يتضح أن التوصية الأهم في هذا الصدد تكمن في ضرورة توطين التكنولوجيا والتقنيات الفائقة ليس فقط من أجل تضييق "الفجوة الرقمية"، وإنما من أجل تعزيز سياسات وممارسات حماية الأمن بشكل عام، والأمن في بعده السيبراني على وجه الخصوص. فضلًا عن ضرورة بناء قاعدة واسعة من الكوادر الوطنية التي تمتلك درجة متقدمة من الإبداع والابتكار. إذ سيساهم هذين الأمرين في تعزيز قدرة الدولة على تبني استراتيجية من شأنها تعظيم الفرص والقدرات والحد من التحديات والمخاطر.

قائمة المراجع:

1) الشامخ، إيمان. **الحكومات في مواجهة أباطرة التقنية.. هل انتهى زمان الدول وبدأ عصر حكم الشركات؟**، الجزيرة، 18 ديسمبر 2021، متاح على: https://www.ajnet.me/midan/miscellaneous/2021/12/18/%D8%A7%D9%84%D8%AD%D9%83%D9%88%D9%85%D8%A7%D8%AA-%D9%81%D9%8A-%D9%85%D9%88%D8%A7%D8%AC%D9%87%D8%A9-%D8%A3%D8%A8%D8%A7%D8%B7%D8%B1%D8%A9-%D8%A7%D9%84%D8%AA%D9%82%D9%86%D9%8A%D8%A9-%D9%87%D9%84.2024/01/21 ،

2) الكويتي، محمد. الأمن السيبراني في عصر الذكاء الاصطناعي، ترينـدز للبحوث والاستشارات، **اتجاهات استراتيجية (25)**، (نوفمبر 2023).

3) صالح، عطا محمد حسن. **نظرية الأمن القومي في التقاليد الإسرائيلية**، (مصر: رسالة دكتوراه، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، 1981).

[1] Trisha Ray, **The quest for cyber sovereignty is dark and full of terrors**, Observer Research Foundation, 25 May 2020, available at: https://www.orfonline.org/expert-speak/the-quest-for-cyber-sovereignty-is-dark-and-full-of-terrors-66676/, 25/04/2022.

4) عرفة، خديجة. **مفهوم الأمن الإنساني وتطبيقاته في شرق آسيا**، (مصر: رسالة ماجستير، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، فبراير 2006).

5) علام، مها. **الفضاء السيبراني وسيادة الدولة في العلاقات الدولية.. دراسة نظرية بالتطبيق على حالة الولايات المتحدة الأمريكية**، (مصر: كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، 2024).

6) عنتر، أحمد. **الذكاء الاصطناعي.. أبهى صور التفاعل بين البشر والتكنولوجيا**، الجزيرة، 24 ديسمبر 2023، متاح على:

7) https://www.ajnet.me/tech/2023/12/24/%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D8%A3%D8%A8%D9%87%D9%89-%D8%B5%D9%88%D8%B1-%D8%A7%D9%84%D8%AA%D9%81%D8%A7%D8%B9%D9%84-%D8%A8%D9%8A%D9%86.2024/09/04 ،

8) ليم، جيونغكي. **الذكاء الاصطناعي التوليدي: ما هو، وما الميزات التي لا يتمتع بها، وما يمكن أن يمثله للأمم المتحدة**، الأمم المتحدة، 18 يوليو 2023، متاح على: https://www.un.org/ar/208258 ، 2025/02/13.

9) "**الأمن في العلاقات الدولية: بين التنظير والواقع الدولي**"، مجلة العلاقات الدولية، 20 سبتمبر 2023، متاح على: https://irajournal.academy/2023/08/26/security-theory-reality/، 2025/01/11.

10) "**أمن الفضاء الإلكتروني**"، مكتب مكافحة الإرهاب التابع للأمم المتحدة، متاح على:

11) https://www.un.org/counterterrorism/ar/cybersecurity، 2025/03/05.

1) Boulanin, Vincent. Kolja Brockmann & Luke Richards**Responsible Artificial Intelligence Research and Innovation for International Peace and Security**, (Sweden: Stockholm International Peace Research Institute (SIPRI), Stockholm, November 2020).

2) Coleman, Kevin. **Virtual States in Cyberspace increase in size and number**, 15 November 2012, available at: https://defensesystems.com/articles/2012/11/15/digital-conflict-virtual-states.aspx , 5/8/2020

3) Cornish, Paul. Rex Hughes & David Livingstone, **Cyberspace and the National Security of the United Kingdom: Threats and Responses**, (UK: Chatham House Report, March 2009).

4) Copeland, Thomas E. The **Information Revolution and National Security**, (USA: Strategic Studies Institute, Army war College, Pennsylvania, August 2000).

5) Dixon, Joan Broadhurst. & Eric J. Cassidy (Editors), **Virtual Futures: Cyberotics**, (New York: Technology and Posthuman Pragmatism, Routledge, 1998).

6) Escott, Eban. **What are the 3 types of AI? A guide to narrow, general, and super artificial intelligence**, Codbots, 24 October 2017, available at: https://codebots.com/artificial-intelligence/the-3-types-of-ai-is-the-third-even-possible, 13/03/2025.

7) Frey, Thomas. **The Virtual Country**, Futurist Speaker, 5 February 2009, available at: https://futuristspeaker.com/future-scenarios/the-virtual-country/, 20/03/2025.

8) Gu, Hongfei. Data, Big Tech, and the New Concept of Sovereignty, **Journal of Chinese Political Science**, Volume 29, (May 2023).

9) Horowitz, Michael C. Gregory C. Allen, Edoardo Saravalle, Anthony Cho, Kara Frederick and Paul Scharre, **Artificial Intelligence and International Security**, Center for a New American Security, July 2018, available at: https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security, 21/08/2024.

10) Kissinger, Henry A. Eric Schmidt & Daniel Huttenlocher, **the Age of AI and Our Human Future**, (USA: Little Brown and Company, New York, 2021).

11) Kurzweil, Ray. **The Singularity Is Near: When Humans Transcend Biology**, (USA: The Viking Press, New York City, 2005).

12) Nelson, Nate. **Ai-Powered-Cybercrime-Cartels-Asia**, Dark Readings, 10 October 2024, available at: https://www.darkreading.com/threat-intelligence/ai-powered-cybercrime-cartels-asia, 22/03/2025.

13) Nye, Joseph S. **Cyber Power**, (Massachusetts: Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, 2010).

14) Ohagi, Masaya. **Polarization of Autonomous Generative AI Agents under Echo Chambers**, (Japan: Association for Computational Linguistics, Tokyo, 2024).

15) Patterson, Nicholas. **What is Cybersecurity and Why is It Important?**, Southern New Hampshire University, 30 October 2024, available at: https://www.snhu.edu/about-us/newsroom/stem/what-is-cyber-security

16) Picarelli, John T. & Phil Williams, Information Technologies and Transnational Organized Crime.:In David S.Alberts and Daniel S. Papp

(Eds.), **Information Age Anthology: National Security Implications of the Information Age**, (Washington DC: Library of Congress Cataloging-in-Publication Data, Volume II, August 2000).

17) Puscas, Ioana. **AI and International Security... Understanding the Risks and Paving the Path for Confidence Building Measures**, (Switzerland: UNIDIR, 2023).

18) Ray, Trisha. **The quest for cyber sovereignty is dark and full of terrors**, Observer Research Foundation, 25 May 2020, available at: https://www.orfonline.org/expert-speak/the-quest-for-cyber-sovereignty-is-dark-and-full-of-terrors-66676/, 25/04/2022.

19) Shahid, Ehtesham. **The implications of AI for regional security**, Arab News, 30 May 2024, available at: https://www.arabnews.com/node/2519841, 03/09/2024.

20) Singh, P.K. **Maneuver Warfare in Cyberspace**, (USA: Marine Corps War College, Marine Corps University, Marine Corps Combat Development Command, Quantico, 1997).

21) Skiba, Dorota Żuchowska. **Hacktivism**, December 2023, available at: https://www.researchgate.net/publication/377163085_Hacktivism, 15/02/2025.

22) Stanham, Lucia. **Ai-Powered Cyberattacks**, CrowdStrike, 16 January 2025, available at: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/,14/02/2025.

23) Suárez, Amanda. **Why Mexican Cyber-Cartels Threaten U.S. National Security**, Geopolitical Moniter, 24 June 2021, available at:

https://www.geopoliticalmonitor.com/why-mexican-cyber-cartels-threaten-u-s-national-security/, 22/02/2022.

24) Voronkov, Vladimir. A**lgorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes**, United Nations Interregional Crime and Justice Research Institute (UNICRI), available at: https://unicri.org/News/Algorithms-Terrorism-UNICRI-UNOCCT, 18/03/2025.

25) Xiaoguang. Yang & Chen Kaihua, **Artificial Intelligence Risks and Governance from a National Security Perspective**, People's Forum Network – Chinese, 16 July 2024, available at: http://www.rmlt.com.cn/2024/0716/707544.shtml, 19/09/2024.

26) "**Artificial Intelligence Definitions**", Stanford University, September 2020, available at: https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf, 03/09/2024.

27) "**Artificial Intelligence (AI)**", US Department of State, available at: https://www.state.gov/artificial-intelligence/, 05/03/2025.

28) "**EU Artificial Intelligence Act**", Article 3: Definitions, available at: https://artificialintelligenceact.eu/article/3/, 17/01/2025.

29) "**History of artificial intelligence**", Iberdrola Group, available at: https://www.iberdrola.com/innovation/history-artificial-intelligence#:~:text=However%2C%20it%20was%20not%20until,term%20did%20not%20yet%20exist, 02/02/2025.

30) "**Looking into the future: Artificial intelligence and its impact on peace and security in Africa**", Amani Africa Media and Research Services, 12 June 2024, available at: https://amaniafrica-et.org/looking-

into-the-future-artificial-intelligence-and-its-impact-on-peace-and-security-in-africa/, 12/09/2024.

31) "**Security**", Collins Dictionary, available at: https://www.collinsdictionary.com/dictionary/english/security, 11/09/2024.

32) "**The Promising Impact of AI in Software Security**", Intrusion, 03 May 2023, available at: https://www.intrusion.com/blog/the-promising-impact-of-ai-in-software-security/, 19/03/2025.

33) "**What is Cybersecurity**?" America's Cyber Defense Agency, 1 February 2021, available at: https://www.cisa.gov/news-events/news/what-cybersecurity , 12/08/2023.

34) "**What is AI in cybersecurity**?", EC-Council University, available at: https://www.eccu.edu/blog/the-role-of-ai-in-cyber-security/, 13/03/2025.