: https://doi.org/10.25130/tjfps.v2i43.706

P-ISSN: 2312-6639
E-ISSN: 2669-9203

TJFPS
http://tjfps.tu.edu.iq/index.php/politic/index
Tikrit Journal for Political Science
مجلة تكريت للعلوم السياسية
IRAQI Academic Scientific Journals
https://iasj.rdd.edu.iq/journals/

No.43

"مستقبل الأمن العربي في عصر الذكاء الاصطناعي: رؤية استشرافية"

"The Future of Arab Security in the Era of Artificial Intelligence: Strategic Foresight"

Asst. Prof. Dr. Sura Thamer Hadi [a]
Ministry of Higher Education and Scientific Research [a]
https://orcid.org/0009-0004-8742-8815

م. د سرى ثامر هادي * [a]
وزارة التعليم العالي والبحث العلمي
دائرة الدراسات والتخطيط والمتابعة

Article info.

Article history:
- Received 12 Oct.2025
-Received in revised form 10 Dec. 2026
- Accepted 23. Feb. 2026
Final Proofreading 14 Mar. 2026
- Available online: 30. Mar .2026

Keywords:
- Arab Security
- Artificial Intelligence
- Digital Sovereignty
- Hybrid Warfare
- Cyber Security

Abstract: Artificial Intelligence (AI) represents a pivotal turning point in human history, transcending its role as a mere technical tool to become the primary driver in reshaping the concepts of power and security within the Arab sphere. As the gravity of confrontations shifts from traditional battlefields to cyber and algorithmic spaces, complex patterns of hybrid threats have emerged, characterized by rapid speed and anonymity. This shift has placed traditional security systems under a rigorous test of resilience and responsiveness, amid a reality marked by technological dependency and a widening digital divide. The foresight into the future of Arab security necessitates moving beyond classical approaches toward adopting strategies that rely on AI as a fundamental pillar for enhancing national sovereignty. This entails transforming security doctrines from "reactive" to "predictive security and preemptive deterrence" by leveraging Big Data to fortify critical infrastructure. The transition toward a smart Arab security system is no longer a technological luxury but a strategic necessity to ensure stability in an era where risks ignore geographical borders. In this age, wars are governed by digital superiority, and sovereignty is preserved only through the mastery of the algorithm, within future trajectories that balance technological opportunities with the obstacles of collective security integration.

*Corresponding Author: Sura Thamer Hadi, Email: Sura.khafaji@gmail.com, Tel:xxx, Affiliation: Ministry of Higher Education and Scientific Research/ Department of Studies, Planning and Follow-up.

معلومات البحث:

تواريخ البحث:

- الاستلام: 12 تشرين الثاني 2025
- بعد التنقيح 10 كانون الأول 2026
- القبول: 06 شباط 2026
- التدقيق النهائي 30 مارس2026
- النشر المباشر: 30 حزيران 2026

الكلمات المفتاحية:

- الأمن العربي
- الذكاء الاصطناعي
- السيادة الرقمية
- الحروب الهجينة
- الأمن السيبراني

الخلاصة: يمثل الذكاء الاصطناعي اليوم نقطة تحول مفصلية في التاريخ الإنساني، إذ تجاوز كونه مجرد أداة تقنية ليصبح المحرك الأساسي لإعادة صياغة مفاهيم القوة والأمن في الفضاء العربي. ومع انتقال ثقل المواجهات من الميادين التقليدية إلى الفضاءات السيبرانية والخوارزمية برزت أنماط معقدة من التهديدات الهجينة التي تتسم بالسرعة والتواري، مما وضع المنظومات الأمنية التقليدية أمام اختبار حقيقي يتعلق بقدرتها على الصمود والاستجابة، في ظل واقع يتسم بالتبعية التقنية واتساع الفجوة الرقمية، وبروز الحاجة الملحة لتجاوز المقاربات الكلاسيكية نحو تبني استراتيجيات تعتمد على الذكاء الاصطناعي كركيزة أساسية لتعزيز السيادة الوطنية، وتحويل العقيدة الأمنية من رد الفعل إلى الأمن التنبؤي والردع الاستباقي عبر توظيف البيانات الضخمة في تحصين البنى التحتية الحيوية، إذ إن الانتقال نحو منظومة أمنية عربية ذكية لم يعد خياراً تكنولوجياً، بل ضرورة استراتيجية لضمان الاستقرار في عصر لا تعترف فيه المخاطر بالحدود الجغرافية، ولا تُدار فيه الحروب إلا عبر التفوق الرقمي، ولا تُحفظ فيه السيادة إلا بامتلاك القدرة على التحكم في الخوارزمية، ضمن مسارات توازن بين الفرص التقنية ومعوقات التكامل الأمني المشترك.

المقدمة:

يشهد العالم المعاصر تحولاً جذرياً في طبيعة التفاعلات الدولية، إذ أفضت الثورة التكنولوجية الرابعة إلى إعادة صياغة موازين القوى خارج الأطر الكلاسيكية المعهودة، مفرزةً واقعاً تتداخل فيه الجغرافيا السياسية مع الفضـــاءات الرقمية. وفي قلب هذا التحول، يبرز الذكاء الاصـــطناعي ليس كظاهرة تقنية عابرة، بل كمتغير اســـتراتيجي كلي القدرة، اســـتطاع خلخلة المفاهيم التقليدية للأمن القومي وإعادة تعريف الســـيادة الوطنية في القرن الحادي والعشـــرين. وبالنســـبة للمنطقة العربية، التي تعيش في خضـــم تجاذبات جيوســـياســـية معقدة وصـــراعات ممتدة، لم يعد الأمن مجرد حماية للحدود الترابية أو تعزيزاً للترســـانات العســـكرية التقليدية، بل أضـحى مرتبطاً بشكل عضـوي بالقدرة على التحكم في الفضـاء الخوارزمي وإدارة التدفقات المعلوماتية والبيانية الهائلة.

إن التحول المتسارع من مفهوم "القوة الصلبة" إلى "القوة الذكية" القائمة على الخوارزميات ومعالجة البيانات الضخمة، وضع الأمن العربي أمام تحديات وجودية غير نمطية؛ لذا تبلورت الحروب السيبرانية والتهديدات الهجينة التي تتسم بالتواري والسرعة الفائقة، لتجعل آليات الردع الكلاسيكية ومنظومات الدفاع التقليدية في حالة انكشاف استراتيجي أمام هجمات لا تعترف بالحدود المادية. ويفرض هذا الواقع مراجعة شاملة

لمدى جاهزية العقل الأمني العربي في استيعاب استحقاقات العصر الرقمي، لتحديد ما إذا كانت التقنيات الناشئة ستمثل عبئاً إضافياً يعمق من حالة التبعية التقنية، أم أنها ستشكل دافع استراتيجي يتيح الانتقال نحو نماذج أكثر تطوراً واستباقية في التنبؤ بالتهديدات وتفعيل آليات الردع الرقمي، بما يضمن تحويل المخاطر الرقمية الزاحفة إلى فرص حقيقية لتعزيز الصمود وتحقيق الاستقرار الاستراتيجي الشامل.

أهمية البحث: تأسيساً على ما تقدم، يكتسب البحث أهميته من تسليط الضوء على الذكاء الاصطناعي وأثره على الأمن القومي العربي من جانب، وصياغة رؤية استشرافية لمستقبل هذا التأثير من جانب آخر، وإمكانية استثمار الدول العربية لهذه التكنولوجيا لحماية أمنها وإداء دورها في الساحة الدولية.

إشكالية البحث: تتبلور إشكالية البحث في رصد الفجوة الوظيفية بين تسارع وتيرة التقنيات الناشئة وبين آليات الاستجابة الأمنية في المنطقة العربية، بهدف استشراف مستقبل هذا الأمن في بيئة تكنولوجية لا تعترف بالحدود، حيث يبرز تساؤل مركزي: كيف يمكن للمنظومة الأمنية العربية الصمود أمام التهديدات المؤتمتة، وما هي مسارات توظيف الذكاء الاصطناعي لتعزيز القدرات التنبؤية والردعية وبناء منظومة أمنية عربية ذكية؟

فرضية البحث: انطلاقاً من الإشكالية آنفاً تبرز فرضية مفادها: كلما زاد مستوى الدمج المؤسسي والسيادي للذكاء الاصطناعي في المنظومة الأمنية العربية، تضاعفت قدرة هذه المنظومة على امتلاك زمام المبادرة الاستراتيجية وتقليص آثار الفجوة التقنية والتهديدات الهجينة والسيبرانية التي من الممكن أن تتعرض لها.

مناهج البحث: يعتمد البحث منهجية تكاملية تزاوج بين منهج تحليل النظم لفهم تفاعل المنظومة الأمنية العربية مع المدخلات التقنية، وبين المنهج الاستشرافي الهادف إلى استقراء سيناريوهات الصراع والتهديد في العصر الرقمي. وينصهر هذا الإطار ضمن مقترب الواقعية التقنية لتحليل أثر الفجوة الرقمية والتبعية التكنولوجية على جوهر السيادة الوطنية، مما يتيح تقديم رؤية علمية تجمع بين دقة التشخيص لواقع التهديدات الهجينة والسيبرانية، وبين رحابة الاستشراف الاستراتيجي لآليات بناء منظومات أمنية عربية ذكية مستقلة.

هيكلية البحث: سعياً للإجابة على إشكالية الدراسة والتحقق من فرضيتها، تم اعتماد هيكلية منهجية تنتظم في مطلبين متكاملين؛ يركز المطلب الأول على تشخيص التحديات الأمنية العربية في بيئة الذكاء الاصطناعي، وذلك في محورين؛ يتناول أولهما التحول من الحروب التقليدية إلى تحديات الحروب الهجينة والسيبرانية، بينما يحلل ثانيهما أثر الفجوة التقنية العربية على مفاهيم السيادة الأمنية. وانتقالاً من مربع التشخيص إلى استشراف الحلول، يأتي المطلب الثاني ليعرض آفاق التوظيف الاستراتيجي للذكاء الاصطناعي في منظومات الردع العربي، إذ يستعرض المحور الأول آليات توظيف هذه التقنيات في تعزيز منظومات الردع، وصولاً إلى المحور الثاني الذي يطرح سيناريوهات مستقبلية واقعية لبناء منظومة أمنية عربية ذكية ومتكاملة.

المطلب الأول: التحديات الأمنية العربية في بيئة الذكاء الاصطناعي

يُقصد بالتحديات هي تلك الصعوبات والعقبات التي يمكن أن تعترض الاستفادة الكاملة من توظيف الذكاء الاصطناعي للتنبؤ والمراقبة رغم أن هناك ما يثبت قدرته على ذلك. إذ تفرض بيئة الذكاء الاصطناعي واقعاً أمنياً معقداً في المنطقة العربية، حيث تتشابك التقنيات الناشئة مع التهديدات السيبرانية المتقدمة، مما يُوجد تحديات غير مسبوقة تستهدف استقرار الأنظمة الرقمية والسيادة الوطنية، وسعياً لتشخيص التحديات الأمنية المعقدة في البيئة العربية، لا بد من تحليل التحول من الحروب التقليدية إلى الأنماط الهجينة والسيبرانية، ومعاينة أثر الفجوة التقنية في تقويض السيادة الأمنية واستقلالية القرار.

أولاً: الحروب التقليدية وتحديات الحروب الهجينة والسيبرانية

تشهد البيئة الأمنية الدولية المعاصرة تحولاً جذرياً في فلسفة الصراع المسلح، إذ لم يعد الميدان المادي الجغرافي هو الساحة الوحيدة لحسم النزاعات، بل تداخلت الأبعاد الرقمية والخوارزمية لتعيد تعريف مفهوم القوة والردع الاستراتيجي. وأضحى الانتقال من الحروب التقليدية التي تعتمد على المواجهة المباشرة بين الجيوش النظامية إلى أنماط الحروب الهجينة والسيبرانية المعززة بالذكاء الاصطناعي هي سمة الحروب الحديثة، مما يفرض على المنطقة العربية تحديات غير مسبوقة تمس جوهر الأمن القومي، حيث يتم استبدال القوة النارية الكثيفة بدقة الخوارزميات وسرعة الأتمتة.[1] وهو ما يطلق عليه تسمية الحرب الهجينة (hybrid warfare) التي تُشير إلى نمط من الصراع المعقد، يجمع بشكل متزامن ومنسق بين العمليات العسكرية النظامية، الهجمات السيبرانية، الدعاية الإعلامية، الضغوط الاقتصادية، وتوظيف فاعلين غير نظاميين مثل المرتزقة أو الجماعات المسلحة، بما يهدف إلى زعزعة استقرار الخصم وإرباكه دون اللجوء إلى مواجهة شاملة تقليدية. [2] وبذلك تعد الحرب الهجينة شكل من أشكال الحرب غير المتكافئة يقوم فيه طرف معين بتنويع الأدوات القتالية وغير القتالية العسكرية التقليدية، الاعمال الإرهابية والأنشطة الالكترونية بصورة منسقة لتحقيق التأثير الأعظم على الخصم

[1] Muhammad Sanaullah Khan, Farhat Asghar Rana, Zoha Irfan, "Hybrid Warfare in the Digital Age: Cyberpower, AI, and the future global security", **Advance Social Science Archive Journal**, Vol.04 No. 01 (July-September 2025), p.3053.

[2] عبد القادر الفرساوي، "الحروب الهجينة والرمادية وعلاقتها بالجماعات الإرهابية"، **مجلة قضايا التطرف والجماعات المسلحة**، المجلد (٦) العدد (٢٠)، (المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا: آب ٢٠٢٥)، ص١٢١.

بهدف تجنب الاشتباك المباشر معه في ميدان قوته بل تسعى لاستنزاف وتعطيل قدراته في مناطق ضعفه، وتصبح الساحة الرئيسية للمعارك هي الإدراك نفسه، حيث يتم توظيف الذكاء الاصطناعي لتوسيع نطاق العمليات النفسية وزعزعة الاستقرار المؤسسي عبر هجمات تستهدف السمعة والمصداقية. [1] وتتميز هذه الحروب بالغموض حيث يطمس الفاعلون المختلطون الحدود المعتادة للسياسة الدولية في الواجهات بين الداخل والخارج والقانوني وغير القانوني، كما تمتاز بصعوبة اسناد الفعل لفاعل محدد لتعمد الطرف المهاجم في إخفاء بصماته باستخدام قوات غير رسمية أو وكلاء محليين، أو هجمات سيبرانية مجهولة المصدر تكون بشن هجمات إلكترونية على البنية التحتية الحيوية (شبكات كهرباء، اتصالات، مصارف) أو استهداف الأنظمة العسكرية للخصم لتعطيلها وإرباكها، وهذا السلاح برز بقوة في كافة النزاعات الهجينة الحديثة. [2]

برز مفهوم الحرب الهجينة بقوة في الخطاب الأمني بعد حرب لبنان ٢٠٠٦، بين (إسرائيل) وحزب الله، إذ لوحظ استخدام أساليب قتالية تقليدية جنباً إلى جنب مع تكتيكات غير نظامية، وحملات التضليل الإعلامي، هذا التكامل بين أدواتٍ متعددة يجعل من هذا الصراع ميداناً حياً لدراسة تطبيقات الحرب الهجينة المعاصرة، [3] ثم الأزمة السورية منذ عام ٢٠١١، التي تعد من أكثر النماذج تعقيداً للحروب الهجينة في التاريخ الحديث، والصراع في ليبيا عام ٢٠١١، بعد سقوط النظام السياسي فيه، تبعهه الصراع في اليمن منذ عام ٢٠١٤، الذي وظفت فيه القوى الإقليمية أدوات الحرب الهجينة، كما شهدت منطقة الخليج العربي هجمات هجينة ركزت على الجانبين السيبراني والاقتصادي دون تبني رسمي من أي دولة، مثل فيروس (شمعون) الذي استهدف شركة أرامكو السعودية وشركات الطاقة في قطر وعُمان استهداف ناقلات النفط في بحر عمان ومنشآت بقيق وخريص التابعة لأرامكو بطائرات مسيرة وصواريخ كروز، إذ تميزت هذه العمليات بـ (الإنكار المعتمد)، حيث صعب إثبات الجهة الفاعلة قانونياً وبشكل قاطع فور حدوثها، وهو جوهر الحرب الهجينة. [4]

---

[1] Aleksandr Shaman, AI’s invisible invasion: how artificial intelligence is becoming the newest weapon in hybrid warfare, research papers, ESCP international politics society, 21 July 2025.

[2] عبد القادر الفرساوي، "الحروب الهجينة والرمادية وعلاقتها بالجماعات الإرهابية"، مصدر سبق ذكره ، ص١٢٢– ١٢٣.

[3] المصدر نفسه ، ص ١٢١ – ١٢٤.

[4] اسلام عبد المجيد عيد، الحرب الهجينة: صورة أخرى للصراع في الشرق الأوسط ما بعد عام ٢٠١١، منصة الجيوسياسية، ٢٠٢١/٣/٢٨، https://www.wgi.world/alharb-alhajinat-surat-ukhraa-lilsirae-fi-alshr-al-awsat-ma-2011/?lang=ar

إذاً، فالهجمات السيبرانية قد تسبق هجوماً برياً لتعمية أنظمة دفاع العدو، والدعاية الإعلامية تواكب العمليات العسكرية لتبريرها أو بث الفرقة في صفوف العدو، إلى جانب تحريك خلايا إرهابية نائمة لتنفذ تفجيرات تشتيتية، وإن هذا التنوع والتزامن يجعل الحرب الهجينة أشد تعقيداً من الحرب التقليدية، ويتطلب تصدياً متعدد المستويات. وفي ذات الوقت، يحقق للمعتدي مكاسب كبيرة بكلفة ومخاطر أقل مقارنة بخوض حرب شاملة، إذ يمكنه إنكار تدخله المباشر وتحاشي استعداء الرأي العام الدولي، فيما يبقى الضرر الناجم عند الخصم حقيقياً وملموساً. [1]

إن توظيف الذكاء الاصطناعي في الحروب الهجينة أدى إلى ظهور نمط جديد يسمى "الحرب الهجينة الخوارزمية"، يتم فيها أتمتة الهجمات السيبرانية باستخدام برمجيات خبيثة تكييفية (مثل هجمات شمعون)، وتحويل حرب المعلومات عبر تغذية نظم المراقبة العاملة بالذكاء الاصطناعي، بمعلومات مضللة بشكل منهجي، مما يحول هذه النظم إلى عملاء مزدوجين آليين دون قصد من مشغليها. وتحسين الضربات الحركية عن طريق الكشف الذكي عن الأهداف وتجسد ذلك في استخدام منظومات الذكاء الاصطناعي كمنظومة (الانجيل) و(لافندر) في عمليات الاغتيال واستهداف القيادات والبنى التحتية في غزة ولبنان، هذا التآزر يهيئ بيئة تهديد غير متكافئة، حيث السرعة والنطاق والغموض الاستراتيجي غير مسبوقة، مما يعطل استراتيجيات الردع التقليدية القائمة على التهديد بالانتقام ويثير مخاوف جدية حول تآكل الخصوصية وحقوق المواطنين الأساسية. [2]

أصبحت المعرفة التقنية، لاسيما في مجالات تعلم الآلة والخوارزميات، هي رأس المال العسكري الجديد، لما يوفره الذكاء الاصطناعي من مزايا تشغيلية مثل تحسين دقة الاستهداف وتقليل المخاطر على الكوادر

---

[1] عبد القادر الفرساوي، مرجع السابق، ص ١٢١ – ١٢٤.

[2] اوسوندي أ. أوسوبا ووليام ويلسر الرابع، "مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل"، منظور تحليلي، مؤسسة RAND، ٢٠١٧، ص١٠. ويُنظر أيضاً:

Muhammad Sanaullah Khan, Farhat Asghar Rana, Zoha Irfan, "Hybrid Warfare in the Digital Age: Cyberpower, AI, and the future global security", 3055

البشرية. [1] ومن يمتلك القدرة على تفكيك تكنولوجيا العدو عبر الهندسة العكسية [2] يكتسب رأسمالاً رمزياً وقوة استراتيجية تمكنه من مقاومة ما يسمى بـ (الاستعمار الرقمي)، [3] مثل نجاح إيران في اسقاط طائرات مسيرة أمريكية و(إسرائيلية) متطورة مثل (RQ−170) و(هرمس) وتفكيكها لإنتاج نسخ محلية الصنع مستنسخة عنها، وإن هذا الدمج بين الذكاء الاصطناعي وأنظمة القيادة والسيطرة أدى إلى بروز حقبة جديدة من النزاعات المسلحة تُعرف بـ (الحروب الفائقة)، التي تتم فيها معالجة البيانات واتخاذ القرارات القتالية بسرعة تقاس بالأجزاء من الثانية تتجاوز قدرة العقل البشري على الاستيعاب أو الرد في الوقت الحقيقي، إذ يتحول فيها الإنسان من قائد في الميدان إلى مراقب للعملية، مما يضع الجيوش العربية التقليدية أمام تحدٍ يتمثل في عجز الاستجابة البشرية؛ فالخوارزميات التي تدير أسراب الطائرات المسيرة(Drone Swarms) أو الصواريخ ذاتية التوجيه تملك قدرة على المناورة وتجاوز الدفاعات الجوية الكلاسيكية، وهذا يجعل فكرة الحشود العسكرية التقليدية عرضة

---

[1] ناصر بن ناصر، "أثر الذكاء الاصطناعي على الأمن الإقليمي وتصورات الهديدات، ومبادرة انشاء منطقة الشرق الأوسط كمنطقة خالية من أسلحة الدمار الشامل"، (معهد الأمم المتحدة لبحوث نزع السلاح: ٢٠٢٥)، ص١٢.
https://unidir.org/wp-content/uploads/02/2025/UNIDIR_The_Impact_of_Artificial_Intelligence_on_Regional_Security_AR.pdf

[2] **الهندسة العكسية Reverse Engineering** أو Engineering Back: وهي عملية تفكيك البرامج والآلات والطائرات والهياكل المعمارية أو الأنظمة لفهم هيكليتها وكيفية عملها دون امتلاك الكود المصدري، وفي كثر من الأحيان تتضمن تفكيك المكونات الفردية للمنتجات الأكبر حجماً، للتمكن من تحديد كيفية تصميم جزء ما لتسهيل إعادة إنشائه، وغالباً ما تستخدم الشركات هذا النهج عند شراء جزء بديل من الشركة المصنعة للمعدات الأصلية (OEM)، لاكتشاف الثغرات الأمنية، وتحليل البرمجيات الخبيثة، وفهم الآليات الدفاعية. بالاعتماد على أدوات التفكيك (Disassemblers) ومصححات الأخطاء (Debuggers) لتحويل كود الآلة إلى لغة مفهومة (IDA Pro, Ghidra). وسُميت عملية الهندسة العكسية على هذا النحو لأنها تتضمن العمل للخلف او بالعكس خلال عملية التصميم الأصلية. يُنظر:
Vimukthi Wanigathunga, "**Reverse Engineering & How it Approach into Cyber Security**" Research Gate: November 2020), p.7.

[3] **الاستعمار الرقمي** Digital Colonialism: هو هيمنة شركات التكنولوجيا الكبرى (Big Tech) والدول المتقدمة على البنية التحتية والبيانات الرقمية للدول النامية، مستخدمة إياها كأدوات ناعمة للسيطرة، استخراج الموارد (البيانات)، والتربح منها. يتخفّى هذا النوع من الاستعمار وراء الخدمات المجانية، ويحوّل المجتمعات المستهدفة إلى مستهلكين تبعيين بدلاً من منتجين للمعرفة الرقمية. لمزيد من التفاصيل يُنظر: حسن علي محمد، ثلاثية الاستعمار الرقمي، **مجلة بحوث الإعلام الرقمي**، العدد (١٠)، (جامعة السويس، كلية الاعلام وتكنولوجيا الاتصال: كانون الثاني/ أذار ٢٠٢٦).

للانكشاف الاستراتيجي التام. [1] وهذا ما حدث في هجمات المسيرات والصواريخ المنسقة والنائية التي استهدفت منشآت أرامكو السعودية عام 2019، إذ تعتمد بعض الدول العربية على أنظمة أمنية ودفاعية مستوردة سواء من الغرب أو الشرق تحولت فيها الهندسة العكسية من مجرد تقنية محايدة إلى رمز سياسي وثقافي للمقاومة في زمن الحروب الرقمية، بهدف كسر احتكار القوى الكبرى للتكنولوجيا، عِبر سعي دول محورية مثل جمهورية مصر العربية، المملكة العربية السعودية، والإمارات العربية المتحدة إلى توطين التكنولوجيا الدفاعية عن طريق بوابة الهندسة العكسية، إذ لم تعد هذه التقنية مجرد وسيلة للاقتباس التقني، بل تحولت إلى استراتيجية أمنية لكسر الاحتكار الدولي وفحص الأنظمة المستوردة لضمان خلوها من الثغرات السيادية. [2]

كشفتا المملكة العربية السعودية والإمارات العربية المتحدة في معرض الرياض العالمي للدفاع في عام ٢٠٢٤، ومعرض أبو ظبي الدولي للدفاع في عام ٢٠٢٣، عن العديد من المركبات والطائرات بدون طيار ذاتية القيادة والمزودة بالذكاء الاصطناعي والتي تم انتاجها محلياً، إلى جانب تطبيقات مختلفة للذكاء الاصطناعي بما في ذلك للأغراض العسكرية مثل أنظمة الدفاع الجوي والاستطلاع التكتيكي والدعم اللوجستي والإخلاء الطبي، إلا أنها لا تُعد أنظمة ذكاء اصطناعي بشكل كامل بل بعضها مجرد أنظمة مستقلة، أي أن قدرة النظام على أداء المهام بدرجات متفاوتة من الاستقلالية دون سيطرة بشرية مباشرة وفق قواعد وشروط محددة مسبقاً، على عكس الذكاء الاصطناعي الذي يتيح للآلات الاستجابة بشكل تفاعلي مع البيئات المتغيرة. وعلى الرغم من أن هذه الأنظمة والتقدم يغيران طبيعة النزاع إلا أنهما لم يؤديا بعد تغييرات في العقائد العسكرية لدول المنطقة العربية، وليس هناك رد فعل واضح على هذه الاستخدامات من جانب دول أخرى في المنطقة. [3] ما يبقي المنطقة العربية سوقاً مربحاً لأسلحة الأعضاء الدائمين في مجلس الأمن والدول الأوربية الكبرى وفقاً لبيانات نقل الأسلحة التابعة لمعهد (ستوكهولم الدولي لأبحاث السلام SIPRI) الذي بينَ إن (٧) من بين أكبر (٢٥) دولة مستوردة للأسلحة في العالم بين عامي ٢٠١٧-٢٠٢١ من دول الشرق الأوسط وهي (مصر،

---

[1] James Johnson, "**Artificial Intelligence and the Future of Warfare: The USA, China, and Strategic Stability".** (Oxford: Oxford University Press: 2021).

[2] فادي علي رضا، الهندسة العكسيّة للذكاء الاصطناعي في الحروب الحديثة: مقاربة سوسيولوجيّة عسكريّة، **مجلة أوراق ثقافية**، العدد (٣٨)، (دار الأمير للثقافة والعلوم، لبنان: ٢٠٢٥/٧/١٦)، ص١٨٩.

[3] ناصر بن ناصر، "أثر الذكاء الاصطناعي على الأمن الإقليمي وتصورات التهديدات، ومبادرة انشاء منطقة الشرق الأوسط كمنطقة خالية من أسلحة الدمار الشامل"، مصدر سبق ذكره ، ص١٥- ١٦

العراق، (إسرائيل)، قطر، المملكة العربية السعودية، تركيا، الامارات العربية المتحدة). [1] وهذا يُسهم في تعقيد استراتيجيات الردع العربي القائم على عدو واضح المعالم ألا وهو الفاعلين من غير الدول (الجماعات المسلحة أو الإرهابية) الذين تتيح لهم التقنيات الناشئة امتلاك قدرات تقنية موازية للدول متمثلة بهجمات التضليل الممنهجة باستخدام تقنيات (التزييف العميق Deepfakes) [2] والمنصات المؤتمتة التي تستهدف تفتيت الجبهة الداخلية، والتلاعب بالرأي العام، وزعزعة الثقة في المؤسسات الأمنية، وتكمن خطورة هذا النوع من الحروب في صعوبة الإسناد مما يجعل المنطقة العربية من أكثر المناطق تأثراً بـ (الحروب الهجينة Hybrid Warfare)، التي توظف الذكاء الاصطناعي لضرب الاستقرار من الداخل دون إعلان رسمي للحرب. [3] ويجعل الفضاء السيبراني العربي مسرحاً لعمليات تخريبية تستهدف (الأعصاب الحيوية) للدولة تتسم بالقدرة على التخفي الطويل داخل الأنظمة، مما يجعل الأمن القومي العربي في حالة استنفار دائم لمواجهة تهديدات غير مرئية قد تؤدي إلى شلل وطني كامل في أوقات التأزم. [4] مما يحول التهديدات السيبرانية من مجرد نشاطات ضارة إلى تحديات وجودية عابرة للحدود، قادرة على تعطيل المصالح الاقتصادية وشبكات البنى التحتية الحيوية، وهو ما يفتح الباب أمام الفواعل من غير الدول لامتلاك أدوات تأثير تضاهي قدرات الدولة التقليدية.

---

[1] Lauriane Héau and Giovanna Maletta, "Arms Transfer and SALW Controls in the Middle East and North Africa: Challenges and State of Play", Stockholm International Peace Research Institute, 1 November 2022, https://www.sipri.org/commentary/topical-backgrounder/2022/arms-transfer-and-salw-controls-middle-east-and-north-africa-challenges-and-state-play

[2] التزييف العميق: تُعد هذه التقنية إحدى أكثر الابتكارات التكنولوجية تطوراً وإثارة للجدل في العصر الرقمي، إذ تعتمد هذه التقنية على الشبكات العصبية التوليدية التنافسية (GANs) لتوليد محتويات مرئية وسمعية مزيفة تحاكي الواقع بدقة يصعب تمييزها عن الحقيقة، وقد اكتسبت هذه التقنية اهتماماً واسعاً نظراً لتداعياتها الخطيرة على مجالات متعددة، أبرزها الإعلام، السياسة، والأمن السيبراني. يُنظر: عرض كتاب: (علي فرجاني، "**التزييف العميق وتقنيات الخداع الرقمي – دراسة متعمقة في التحديات المهنية والتقنية**، دار السحاب للنشر والتوزيع: القاهرة، ٢٠٢٤)، في: **مجلة اتجاهات سياسية**، المجلد (٨)، العدد (٢٩)، (المركز الديمقراطي العربي، ألمانيا: كانون الأول ٢٠٢٤)، ص٨٤.

[3] منيرة العتيبي، "**الذكاء الاصطناعي في الشؤون العسكرية: تحولات العقيدة والردع**"، (مركز الملك فيصل للبحوث والدراسات الإسلامية، الرياض: 2023). ويُنظر أيضاً:

Kenneth Payne, "Warbot: The Dawn of Artificially Intelligent Conflict", (Hurst & Company, London: 2021).

[4] Paul Scharre, "Four Battlegrounds: Power in the Age of Artificial Intelligence" (W. W. Norton & Company, New York: 2023), p.156.

إن هذا التعقيد في المشهد الرقمي، وتنامي قدرات الفواعل ما دون الدول، لا ينفصل عن واقع الفجوة التقنية التي تعاني منها المنطقة العربية، وهو ما يستدعي فحص أثر هذا التفاوت في تقويض السيادة الأمنية.

ثانياً: إشكالية الفجوة التقنية العربية على السيادة الأمنية

ترتبط السيادة في العصر الرقمي بمدى القدرة على امتلاك التكنولوجيا لا مجرد استهلاكها. وتمثل الفجوة التقنية بين الدول العربية والمراكز العالمية لإنتاج الذكاء الاصطناعي (الولايات المتحدة، الصين) تحدياً وجودياً للأمن القومي العربي يعيد تعريف مفهوم الاستقلال الأمني والسياسي. إذ إنها لا تقتصر على التفاوت في امتلاك الأجهزة والعتاد، بل تمتد لتشمل القدرة على إنتاج المعرفة والتحكم في البيانات والسيادة على الفضاء السيبراني.

ظهر مصطلح (السيادة الرقمية Digital Sovereignty) بوصفه تعبيراً عن حق الدول في التحكم ببياناتها الرقمية وشبكاتها المعلوماتية وأمنها السيبراني. [1] ويُشير (كلاوس شواب Klaus Schwab) إلى ان (السيادة الرقمية) هي قدرة الدولة على تقرير مصيرها في العالم الرقمي بنفس القدر الذي تمارسه في العالم المادي. [2] كما يرى (جوزيف ناي) أن الفضاء الرقمي أوجد شكلاً جديداً من "تآكل السيادة" لأن الدولة لم تعد الطرف الوحيد القادر على التحكم في التدفقات العابرة للحدود، في ظل وجود شركات التكنولوجيا العملاقة، وهنا تعني السيادة القدرة على بناء شبكات من القواعد والمؤسسات للتحكم في التدفقات الرقمية وتقييد المخاطر. [3]

استناداً إلى المفهوم آنفاً، تسارعت دول العالم نحو إدراج الابتكارات الإلكترونية ضمن سياسات الأمن القومي، في حين افتقرت الخطط الاستراتيجية والمستقبلية لغالبية الدول العربية لهذا الدمج، مما أدخلها في تبعية تكنولوجية وفجوة رقمية مزدوجة (داخلية وخارجية)، [4] ويتجلى هذا الانكشاف في الاعتماد الكلي أو الجزئي على استيراد التقنيات الأجنبية لتشغيل المرافق العامة، والشبكات السلكية واللاسلكية، والمنصات

---

[1] ايمن عمر، "**أثر التكنولوجيا على نظريات الجغرافيا السياسية (الفضاء السيبراني باعتباره إقليم جديد)**"، دراسات بحثية، (المركز الديمقراطي العربي، ألمانيا: ١٨ تموز ٢٠٢٥)، ص ٧٦٩.

[2] Klaus Schwab, **"Shaping the Future of the Fourth Industrial Revolution"**, World Economic Forum, 2018, p.132.

[3] Joseph S. Nye, "Power in the Cyber Age", (Oxford University Press: 2017), p. 49.

[4] بهاء عدنان السعبري وعماد عبد خضير الزرفي، "العناصر التقنية للتهديد الالكتروني"، **مجلة مركز دراسات الكوفة**، العدد ٥٧، (النجف: ٣٠ حزيران ٢٠٢٠)، ص٤٣٥.

الاتصالية والفضائية؛ الأمر الذي استباح أمنها السيادي وقوّض قدرتها على إدارة شؤونها الأمنية والخدمية بشكل مستقل، برغم وجود مؤشرات مغايرة نسبياً في دول الخليج العربي التي تحاول توظيف التكنولوجيا في حوكمة مؤسساتها. [1]

من الجدير بالذكر هنا أن الخوارزميات التي تدير أجهزة الاستخبارات أو أنظمة الدفاع غير معلومة الكود المصدري للطرف المشتري، لإن معظم أنظمة التشغيل والحماية التي تعتمد عليها الدول العربية هي أنظمة خارجية وليس وطنية. مما يُثير تساؤل حول ما قد تزرعه الدول المصنعة، يتيح لها مراقبة العمليات الأمنية العربية أو تعطيل الأنظمة في لحظات الصِدام الجيوسياسي، وهو ما يفرغ مفهوم السيادة من محتواه الحقيقي، كونه يضع كميات هائلة من البيانات الأمنية والاجتماعية العربية تُعالج وتُخزن في خوادم تابعة لشركات تقنية كبرى تخضع لقوانين دولها الأم، مما يؤدي إلى ما يُسمى بـ (الاستعمار الرقمي)، وفيه تمتلك القوى الخارجية القدرة على تحليل السلوك المجتمعي والأمن العربي، واستخدام هذه التحليلات في التنبؤ بتحركات الدولة أو هندسة أزمات داخلية، مما يجعل الأمن العربي مكشوفاً رقمياً أمام القوى التي تملك القدرة الحاسوبية العالية.[2]

بالوقت الذي تواجه فيه الدول العربية تحديات الانكشاف على منصات أجنبية غير خاضعة للقوانين المحلية مثل (Facebook, Google, TikTok) مما يهدد الخصوصية ويؤثر على الأمن الفكري والثقافي، لاسيما في ظل هشاشة الثقافة الرقمية لدى الافراد والمؤسسات فضلاً عن نقص الكفاءات المتخصصة في علم البيانات والأمن السيبراني. ولاتزال العديد من الدول العربية تفتقر لتشريعات شاملة تنظم الفضاء الرقمي وتحاسب على الجرائم الالكترونية، بالوقت الذي تستغل فيه الجماعات الإرهابية هذا الفضاء للتجنيد ونشر الأيديولوجيات وتمويل الأنشطة والتضليل السياسي والابتزاز ونشر الفوضى باستخدام (التزييف العميق Deepfake). [3]

تؤكد المعطيات أن المجتمع العربي ما زال مستهلكاً رقمياً يفتقر لإنتاج البرمجيات والمكونات الصلبة، بالتزامن مع ضعف البيئة والخبرة القانونية المتخصصة ونقص التأهيل الجامعي؛ مما أنتج واقعاً تفتقر بنيته

---

[1] المصدر السابق، ص٤٣٤.

[2] محمد الرميحي، "**الأمن القومي العربي في عصر الرقمنة: التحديات والفرص**"، (مركز دراسات الوحدة العربية، بيروت: 2024).

[3] هيثم جبار طه، "التحديات الأمنية التي تواجه الدول العربية في مجال السيادة الرقمية"، وكالة الحدث الإخبارية، ٥ آب ٢٠٢٥. https://www.alhadathcenter.net/index.php/views/ 23-55-14-05-08-2025-145576

للمجانسة مع المعايير الدولية، وعرّض الكيانات العربية للهجمات السيبرانية من فاعلين نظاميين ودول معادية، [1] وفي ظل هذه السطوة التكنولوجية، تبرز الحاجة لتأطير استراتيجية قومية شاملة تواكب الطفرة المعلوماتية، وتضمن حماية الفضاء الرقمي وتوظيفه إيجابياً في صناعة القرار، [2] إذ لم تعد القوة العسكرية والاقتصادية المحددات الوحيدة لوزن الدول الجيوسياسي، بل أُضيفت إليها "القوة السيبرانية" بوصفها ركيزة السيادة الرقمية الشرطية للحفاظ على السيادة الوطنية التقليدية.

المطلب الثاني: آفاق التوظيف الاستراتيجي للذكاء الاصطناعي في منظومات الردع العربي

إنّ توصيف التحديات السيبرانية والأنماط الهجينة للصراعات المعاصرة، يفرض بالضرورة التوجه نحو مقاربة أمنية أكثر حداثة؛ إذ لم يعد الذكاء الاصطناعي مجرد خيار تقني، بل أصبح ركيزة جوهرية لإعادة صياغة مفاهيم الردع والتنبؤ. وقد باتت الدول العربية اليوم في قلب هذا التحول التكنولوجي، حيث تفرض البيئة الأمنية الإقليمية المعقدة في المنطقة العربية ضرورة الانتقال من مفهوم الأمن التقليدي القائم على الحشود العسكرية، إلى مفهوم الأمن الذكي المستقل، لاسيما مع تعرض المنشآت الحيوية العربية لاختبارات أمنية غير مسبوقة وضعت الجاهزية الدفاعية تحت مجهر التقييم الخوارزمي. ومن هنا، تبرز الحاجة لاستكشاف آفاق التوظيف الاستراتيجي لهذه التقنيات، وتفكيك سيناريوهات بناء منظومات دفاعية ذكية قادرة على تحويل التهديدات الرقمية إلى فرص لتعزيز الصمود الاستراتيجي وتحقيق السيادة التقنية المنشودة.

أولاً: توظيف الذكاء الاصطناعي في آليات الردع

في ظلّ تنامي المخاطر السيبرانية والتقدّم في الأسلحة الاستراتيجية عالية الدقّة مثل الصواريخ فوق الصوتية (Hypersonic Missiles)، تطوّر مفهوم الردع الكلاسيكي المستند إلى نظرية توازن الرعب النووي ليشمل استراتيجياتٍ جديدة تصبّ في مجال "الردع السيبراني" أو "الردع متعدد الأبعاد" الذي يزاوج بين الإمكانات النووية وتقنيات التشويش والمعلوماتية. فأصبح يتطلّب الردع حالياً الآتي:

1. **بناء التحالفات التقنية (Tech Alliances) للإنذار المبكر والردع متعدد الأبعاد:** يتطلب الردع الحديث ربط البنى التحتية الرقمية العربية لضمان الاستجابة الجماعية الفورية ضد التهديدات الفائقة، وتوظيف الأنظمة

[1] بهاء عدنان السعبري وعماد عبد خضير الزرفي، "العناصر التقنية للتهديد الالكتروني"، مصدر سبق ذكره ، ص٤٣٥– ٤٣٦.
[2] المصدر نفسه ، ص٤٣٦.

الذكية لمواجهة الأسلحة الاستراتيجية عالية الدقة كالصاروخية والجوية،)مثل مشروع "سندباد" والتعاون التقني الخليجي–الأمريكي المشترك لربط أنظمة الرصد المبكر بمستشعرات خوارزمية لمراقبة الأجواء. [1]

2. **تطوير منظومات القيادة والسيطرة المعرفية الذكية:** كركيزة استراتيجية لتعزيز صلابة الدولة، وحماية فضائها السيادي، وترسيخ قدرتها على الردع والاشتباك مع التهديدات بأدوات متعددة، لا تُحصّن فقط أمنها الوطني، بل تُعيد ترسيخ مكانتها كفاعل مستقل ضمن النظامين الإقليمي والدولي. [2] إذ لم تَعُد منظومات الدفاع مجردَّ بُنى تسليحية معزولة، بل أصبحت منظومات معرفية تدمج أدوات الفضاء، والرصد السيبراني لتأمين الإنذار المبكر واللحظي لصانع القرار في التعامل مع التهديدات المتزامنة بأقل تكلفة وأعلى كفاءة. وعن طريق تطبيق مبدأ (انعدام الثقة الرقمي) تتحول الدولة إلى كيان دفاعي مرن، لا يقتصر ردعه على الخصم الخارجي، بل يشمل حماية بُنيته الداخلية من الاختراق، مثل توجه مراكز الأمن السيبراني الوطني في السعودية والإمارات لتبني أنظمة دفاع ذكية تعتمد الأتمتة الكاملة لرصد التهديدات في أجزاء من الثانية. [3]

3. **كسر الفجوة التكنولوجية والاعتماد على الذكاء الاصطناعي:** يؤدي تباين القدرات الفضائية الإقليمية إلى فجوة تشغيلية تمنح الأطراف المتقدمة مزايا الإنذار المبكر ودقة الاستهداف، في مقابل انكشاف الدول العربية للمراقبة المستمرة، وافتقارها لآليات التحقق الوطني من تحركات الخصوم، وارتهانها للمعلومات الخارجية التي تقيد خياراتها الاستراتيجية. ويتعاظم هذا الانكشاف مع تصاعد التهديدات الهجينة التي تفرض الانتقال إلى نظم دفاعية متكاملة تدمج المكونات التقنية بالتنظيمية لحماية السيادة الإقليمية. [4] وضمن هذا المسار، يمثل تجنيد الذكاء الاصطناعي عسكرياً رافعة استراتيجية تتيح للدول العربية كشف دفاعات الخصوم والتحقق من تحركاتهم

---

[1] ايمن عمر، "أثر التكنولوجيا على نظريات الجغرافيا السياسية (الفضاء السيبراني باعتباره إقليم جديد)"، مصدر سبق ذكره ، ص٧٦٠.

[2] Lockheed Martin. Layered Defense, Orbital Advantage: The Space Domain's Rising Role. 11 Aug. 2025, https://www.lockheedmartin.com/en-us/news/features/2025/layered-defense-orbital-advantage-the-space-domains-rising-role.html

[3] NATO, "NATO Integrated Air and Missile Defence Policy" 13 Feb. 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-integrated-air-and-missile-defence-policy

[4] مركز الإمارات للدراسات والبحوث الاستراتيجية. "تعزيز ركائز الدولة الوطنية في الشرق الأوسط: الإشكاليات الراهنة والاستراتيجيات المقترحة." ص٣٢. تمت الزيارة بتاريخ ٢٠٢٦/٣/٣. https://www.ecssr.ae/ar/research-products/periodic-studies-203833/3/1

بقدرات وطنية منخفضة التكلفة، فضلاً عن تقليل مخاطر مواجهات المناطق المحرمة، وإجبار الأعداء على استنزاف مخزونهم العميق من الذخائر. [1]

4. **تطوير أدوات الردع الفضائي والتشويش الكهرومغناطيسي الذكي:** أصبح من الضرورة أن تعمل الدول لاسيما العربية على تطوير أدوات للردع الفضائي، على سبيل المثال الأسلحة المضادة للأقمار الصناعية (ASAT)التي لها القدرة على تدمير الأقمار أو تعطيل وظائفها، وتتيح للدول شلّ قدرات خصومها العسكرية والاتصالية، عِبر تقنيات التشويش الكهرومغناطيسي كوسيلة فعالة لتعطيل الإشارات بين الأقمار ومحطاتها الأرضية، دون الحاجة للاشتباك المباشر. [2]

5. **تحصين الخوارزميات ضد الانحيازات الأيديولوجية والعنصرية التاريخية لمطوريها:** حماية الأمن العربي تتطلب بناء قواعد بيانات وطنية لتدريب الخوارزميات العسكرية، لتجنب خطر الاعتماد على تصاميم خوارزمية غربية أو خارجية تحمل أطراً قيمية أو أيديولوجية قد تصنف التهديدات بشكل منحاز وضار بالمصالح العربية، لاسيما أن هناك مخاوف من خطر توظيف البيانات المستندة إلى الخوارزميات بسبب العنصرية التاريخية والنظامية والمؤسسية. لأن البيانات المدنية والعسكرية المستخدمة لتدريب الخوارزميات قد تكون متحيزة بطبيعتها، وبالتالي فإن أدوات تقييم المخاطر، التي تعتمد على هذه البيانات، ممكن أن تتأثر بشكل غير متوازن بالأطر القيمية والأيديولوجية لمطوريها. [3]

6. **صياغة استراتيجية أمنية وقانونية عربية موحدة لفضاء الذكاء الاصطناعي:** أن قيام الدول العربية بإصلاح ثغراتها بنفسها أو سن قوانين وتشريعات رادعة فالإطار القانوني المنظم يشكل شرطاً أساسيّاً لتحقيق الاستقرار السياسي والاجتماعي وضمان حماية الحقوق والالتزامات، بما يُعزز من ثقة المؤسسات والمواطنين في النظام

---

[1] ليث عصام مجيد العبيدي، "الذكاء الاصطناعي والوجود الإنساني: قراءة فكرية في الابعاد العسكرية"، **المجلة السياسية الدولية**، العدد ٥٨، (الجامعة المستنصرية: ١ اذار ٢٠٢٤)، ص٤١٦.

[2] ايمن عمر، "أثر التكنولوجيا على نظريات الجغرافيا السياسية (الفضاء السيبراني باعتباره إقليم جديد)"، مصدر سبق ذكره ، ص٧٧٠

[3] ليث عصام مجيد العبيدي، "الذكاء الاصطناعي والوجود الإنساني: قراءة فكرية في الابعاد العسكرية "، مصدر سبق ذكره ، ص٤١٨.

السياسي. [1] كما لا بُد من بناء استراتيجية أمنية توحد الجهود والتعاون بين الدول من أجل إرساء فضاء سيبراني آمن ومستقر، لتعزيز الثقة بين الدول، ودعم التجارة الدولية، وحماية البنية التحتية الحيوية وتمهيد الطريق لنظام دولي يعتمد على التعاون في مواجهة التهديدات المشتركة بدلاً من التنافس. لذا أصبح من الضرورة تطوير القدرات الدفاعية والاستثمار في تقنيات الذكاء الاصطناعي والتعلم الآلي والاستفادة منه، والمساهمة في تدريب وتأهيل متخصصين في حماية أمن البنى التحتية الحيوية والشبكات الحكومية. [2]

أنَّ فاعلية الردع الحديث لم تعد رهينة القوة العسكرية المادية فحسب، بل باتت ترتكز على امتلاك منظومات ذكية مستقلة قادرة على تجاوز الانحيازات الأيديولوجية الخارجية، وتحصين السيادة الوطنية عبر توازنٍ دقيق بين الابتكار التقني، والتعاون الدولي، والأطر القانونية الملزمة.

ثانياً: سيناريوهات بناء منظومة أمنية عربية ذكية

تشير المؤشرات الاستشرافية إلى أن صناعات الذكاء الاصطناعي والتكنولوجيات التوليدية الفائقة لم تعد تمثل حيزاً تقنياً مضافاً للقدرات التقليدية للدول، بل غدت "متغيراً جيوسياسياً بنيوياً" يعيد إنتاج مفاهيم القوة والسيادة الوطنية من جذورها. وفي ظل هذا الواقع المتسارع، يتأرجح مستقبل الأمن القومي العربي بين منظورين حاكمين؛ منظور واقعي كلاسيكي يرى في الطفرة الخوارزمية تهديداً عابراً للمادة الفيزيائية للدولة يصعب صده، ومنظور استشرافي استباقي يرى في هذه الطفرة الرافعة الاستراتيجية البديلة الكفيلة بإنتاج معادلات ردع مستحدثة تتجاوز الفوارق العسكرية التقليدية. إن هذا التموضع المستقبلي يفرض حتماً ضرورة الانتقال من نموذج الأمن الحمائي الكلاسيكي (القائم على ترصد الاختراقات المادية وحماية الحدود الجغرافية بمنطق رد الفعل المتأخر) إلى نموذج الأمن التنبؤي الاستباقي الخوارزمي (القائم على الأتمتة الكاملة للقرار الأمني، ومعالجة التدفقات البياناتية الضخمة، وإحباط التهديد السيبراني أو العسكري في فضائه الرقمي قبل تمظهره المادي).

وارتباطاً بالمسارات التفاعلية للتطور التقني ومستويات السيولة الأمنية الدولية، تتحدد المآلات المستقبلية للأمن العربي عبر سيناريوهين بنيويين محكومين بمدى القدرة على امتلاك التكنولوجيا أو التكيف معها:

---

[1] مركز الإمارات للدراسات والبحوث الاستراتيجية. "تعزيز ركائز الدولة الوطنية في الشرق الأوسط: الإشكاليات الراهنة والاستراتيجيات المقترحة" مصدر سبق ذكره ، ص٣٨.

[2] محمد محمود زيتون، "العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني"، **المجلة العربية للنشر العلمي**، العدد٧٧، (منظمة المجتمع العلمي العربي، قطر: ٢ آذار ٢٠٢٥)، ص١٧٢ – ١٧٣.

السيناريو الأول: التحول الاستراتيجي نحو منظومة أمنية عربية ذكية

ينطلق هذا السيناريو من فرضية حدوث قفزة نوعية في العقل السياسي والأمني العربي، تُفضي إلى تبني نموذج الأمن التنبؤي الاستباقي كمنظومة إقليمية جماعية وممأسسة، وهو مسار قد يفضي إلى ثورة في عقيدة الأمن الجماعي المشترك وآليات الدفاع عن الأمن القومي. ويتحدد المسار الديناميكي لهذا السيناريو عبر خمس قنوات بنيوية متكاملة:

1. **امتلاك البنية التكنولوجية السيادية:** ويتحقق ذلك بالاستغناء الكامل عن الأطر التقنية والبرمجية الوافدة التي قد تحتوي على ثغرات أمنية كامنة، والعمل على تعزيز الابتكار التكنولوجي المحلي عبر بناء مراكز بيانات عملاقة (Data Centers) مستقلة تُدار بالحوسبة السحابية العربية المشتركة. ويتيح هذا المحدّد تشفير خوارزميات تعلم آلي وطنية خالصة، تمنح المنظومة الأمنية القدرة على رصد الأنماط السلوكية غير النمطية، والتنبؤ بالحركات الإرهابية أو الهجمات السيبرانية قبل تشكلها المادي في أرض الواقع، مما يحول الدفاع إلى نمط "الاستباق الخوارزمي". [1]
2. **عولمة الدفاع السيبراني والردع المرن:** يقوم هذا المحدد على تأسيس منصة إقليمية موحدة لتبادل الاستخبارات الرقمية والإنذار المبكر بشكل لحظي بين الدول الأعضاء. ويتم القياس هنا على المقاربات القائمة بالفعل كـ "مئوية الإمارات 2071" واستراتيجيتها للذكاء الاصطناعي التي تستهدف أتمتة التحليلات الأمنية والخدمات السيادية بنسبة كاملة بحلول عام 2031، وإن تعميم هذا النموذج عربياً سيتيح محاكاة الأزمات المستقبلية المعقدة عبر نماذج تنبؤية دقيقة إحصائياً، تمنع انهيار أي دولة منفردة أمام الحروب الهجينة. [2]
3. **فرض السيادة التشريعية والحوكمة الرقمية:** إذ لا يمكن تفعيل نموذج أمني خوارزمي في ظل فراغ تشريعي؛ الأمر الذي يستدعي العمل على صياغة قوانين موحدة ومشددة تلزم الشركات التكنولوجية العالمية بتخزين البيانات داخل الحدود الوطنية لتوطين البيانات (Data Localization) داخل الحدود الإقليمية العربية،

[1] مركز الإمارات للدراسات والبحوث الاستراتيجية. "تعزيز ركائز الدولة الوطنية في الشرق الأوسط: الإشكاليات الراهنة والاستراتيجيات المقترحة" مصدر سبق ذكره ، ص٦٣.

[2] هيثم جبار طه، "التحديات الأمنية التي تواجه الدول العربية في مجال السيادة الرقمية"، مصدر سبق ذكره .

وإجبار الشركات التكنولوجية الاحتكارية العالمية على الامتثال للسيادة القانونية للدول، مع إنشاء هيئات رقابية مستقلة تمتلك سلطة الردع القانوني والتقني ضد الجرائم المعلوماتية وتزييف التدفقات الإخبارية. [1]

4. **توطين رأس المال البشري التخصصي:** ويرتبط هذا بإنتاج ثورة في المناهج الأكاديمية والبحثية، العسكرية منها والمدنية، بهدف تنشئة جيل من المحللين الاستراتيجيين والمهندسين القادرين على تفكيك شفرات الخوارزميات المعقدة وإدارة الحروب السيبرانية. ويتطلب ذلك هندسة بيئات عمل جاذبة ومميزة مادياً وتقنياً لتأمين هذه العقول ومنع ظاهرة هجرة العقول إلى العواصم الغربية والمصنعة للتكنولوجيا.[2]

5. **مراكز العمليات الأمنية ذاتية المعالجة:** عن طريق الانتقال نحو بناء مراكز عمليات أمنية (Security Operations Centers) متطورة لا تعتمد على الإدخال البشري البطيء، بل تعتمد على أنظمة الدفاع الذاتي (Self-healing systems)، هذه الأنظمة تمتلك القدرة على رصد الهجمات السيبرانية المؤتمتة التي تشنها جيوش برمجية معادية واحتوائها ومعالجتها آلياً في أجزاء من الثانية، مما يحمي البنى التحتية الحيوية كشبكات الطاقة، والاتصالات، والأنظمة المالية من التدمير المفاجئ. [3]

يمثل هذا المسار قفزة جيوستراتيجية تنقل المنطقة من مربع التبعية الرقمية العميقة إلى مربع "السيادة الذكية" القادرة على صياغة شروطها الدولية. ورغم كفاءة هذا السيناريو، إلا أن مآله الاستشرافي يصطدم بكوابح بنيوية تتمثل في بطء التنسيق السياسي التقليدي، وتفاوت الأولويات الأمنية بين العواصم العربية، ومحدودية الثقة في بناء منظومات بيانات مشتركة.

السيناريو الثاني: الاستمرارية التطورية في توظيف الذكاء الاصطناعي أمنياً

ينطلق هذا السيناريو من فرضية بقاء الأطر الأمنية الكلاسيكية المنفصلة كأداة وحيدة لإدارة السيادة الوطنية، مع لجوء كل دولة على حدة إلى إدماج تراكمي، حذر، وبطيء لتطبيقات الذكاء الاصطناعي ضمن

---

[1] محمد محمود زيتون، "العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني"، مصدر سبق ذكره ، ص ١٧٣.

[2] نبيل فهمي، نحو منظومة أمنية عربية وشرق أوسطية، جريدة الشروق، مصر، ١٦ أذار ٢٠٢٦.
https://www.shorouknews.com/columns/view.aspx?cdate=16032026&id=6722429f--4461 4d26-aaaa-e 84357563850

[3] World economic forum, “The global risks report”, 11 January 2023, p.38.
https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

أنظمتها الدفاعية التقليدية دون الوصول إلى سقف الاندماج الإقليمي. ويتسم هذا المسار بالملامح الاستشرافية الإجرائية الآتية:

1. **التحديث التقني القائم على الاستيراد والانكشاف الاستراتيجي:** تستمر الدول في تحسين كفاءة أدواتها الأمنية الداخلية، كأنظمة القيادة والسيطرة ونظم الطائرات المسيرة للمراقبة الحدودية، عبر الاستيراد المباشر للخوارزميات والبرمجيات الجاهزة من الشركات الغربية أو الآسيوية؛ بيد أن المقاربة الاستشرافية تحذر من أنه إذا ما استمر اعتماد هذه الدول على هذه البرمجيات المستوردة، فإن ذلك سيؤدي بالضرورة إلى شلل وطني بنيوي في لحظات الصراع الحرج، فالأمن لا يُبنى بتقنيات الخارج التي تحتوي حتماً على "أبواب خلفية (Backdoors)" تتيح للدول المصنعة تعطيل هذه الأسلحة أو التجسس على القرار الأمني في أوقات الحروب. [1]

2. **محدودية التنسيق التكتيكي وازدواجية الجهود:** يقتصر التعاون الإقليمي في هذا المسار على التنسيق الثنائي المشترك والبروتوكولات النظامية لتبادل بعض البيانات التقليدية. هذا القصور ينتج عنه تكرار مجهد في النفقات والجهود البحثية، ويترك الأمن العربي العام في حالة ضعف بنيوي وتشتت أمام الهجمات والجيوش السيبرانية المنظمة، أو الفاعلين من غير الدول الذين يمتلكون برمجيات هجومية رخيصة ومجهولة المصدر وعابرة للحدود. [2]

3. **التفاوت التشريعي وقصور الحماية القانونية:** بقاء الفجوة التشريعية عميقة بين الدول العربية في تنظيم الفضاء السيبراني، مما يحرم المنطقة من تشكيل جبهة قانونية أو تفاوضية موحدة تفوق قدرة الشركات التكنولوجية العابرة للقارات، ويجعل البيانات السيادية العربية مستباحة ومخزنة في خوادم (Servers) تقع خارج النطاق الجغرافي والقانوني للدول العربية. [3]

---

[1] عمار مراد غركان، التعاون الدولي للتصدي لخطر الإرهاب باستخدام الذكاء الاصطناعي، مستقبل الذكاء الاصطناعي: تحديات قانونية واخلاقية، **مجلة قضايا التطرف والجماعات المسلحة**، المجلد (٦) العدد (١٧)، (المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا: تشرين الثاني ٢٠٢٤)، ص٩٠.

[2] المنظمة العربية لتكنولوجيات الاتصال والمعلومات، " **الرؤية العربية للأمن السيبراني: الواقع – التحديات – الفرص**"، (جامعة الدول العربية، تونس: ٢٠٢١)، ص١٥.

[3] World economic forum, "**The global risks report". Cit.; NAUSS & UNICRI, "1st Artificial Intelligence Forum for Law Enforcement Uses**", (Naif Arab University for Security Sciences: October 2023). 4-5

4. الاستقطاب واتساع الفجوة الرقمية البينية: يفضي هذا السيناريو إلى انقسام البيئة الأمنية العربية عمودياً؛ حيث تنجح دول الفائض المالي (كالخليج العربي) في تبني نماذج الحوكمة الرقمية وأنظمة الرصد الاستباقي، بينما تبقى دول عربية أخرى تعاني من كوابح اقتصادية واضطرابات سياسية في فخ "الفقر البياناتي" والبنى التحتية المتهالكة، مما يحولها إلى ثغرات أمنية يستغلها الخصوم لضرب استقرار الجوار الإقليمي. [1]

بناءً على مؤشرات الواقع الراهن، يُعد هذا السيناريو هو الأكثر ترجيحاً في المدى المنظور؛ كونه يتوافق مع طبيعة التنافس البيني العربي وحرص الدول على الخصوصية الأمنية السيادية. وهو مسار يضمن تحسناً تدريجياً في الحوكمة الأمنية الداخلية لكل دولة على حدة، لكنه بالوقت ذاته يُبقي الأمن العربي العام في منطقة "الانكشاف الاستراتيجي"، وعاجزاً عن تشكيل كتلة ردع جماعية قادرة على مجابهة الحروب الخوارزمية المتطورة مجهولة المصدر.

خاتمة:

إن الصمود في العصر الرقمي ليس مجرد سباق تسلح تقني، بل هو صراع إرادات لامتلاك الخوارزمية التي ستحكم موازين القوى في النظام الدولي الجديد. ولن تتحقق السيادة الوطنية الحقيقية إلا إذا تحول العقل الأمني العربي من مرحلة "رد الفعل" إلى مرحلة "الريادة الرقمية". لإن مستقبل الأمن العربي في عصر الذكاء الاصطناعي مرهون بالقدرة على الانتقال من الاستهلاك التقني إلى الإنتاج المعرفي والسيادي. لإن المعركة القادمة ليست على الأرض، بل هي معركة على الخوارزمية؛ فمن يمتلك القدرة على توجيه الذكاء الاصطناعي سيصيغ مستقبل السيادة، ومن يغيب عن هذا الميدان سيجد نفسه في حالة تبعية رقمية دائمة.

في ضوء ذلك، يمكن تلخيص أبرز الاستنتاجات في الآتي:

1. أن أنظمة الردع الكلاسيكية أصبحت تعاني من عجز الاستجابة أمام الهجمات المؤتمتة وأسراب المسيرات التي تدار بخوارزميات تتجاوز سرعة الإدراك البشري.

2. إن الاعتماد على أنظمة أمنية أجنبية (مغلقة الكود) يمثل ثغرة استراتيجية قد تحول التقنيات المستوردة إلى "عملاء مزدوجين" في وقت الأزمات، مما يجعل (الهندسة العكسية) وتوطين البرمجيات ضرورة أمنية قصوى.

[1] المنظمة العربية لتكنولوجيات الاتصال والمعلومات، " **الاستراتيجية العربية للأمن السيبراني2023-2027**"، (جامعة الدول العربية، تونس: ٢٠٢٣).

3. تبلور الفضاء الرقمي كإقليم سيادي خامس، يتطلب حوكمة قانونية وتشريعية عربية موحدة لسد الفجوة التنظيمية التي تستغلها الجماعات المسلحة والفاعلون من غير الدول.

4. لم يعد كافياً انتظار وقوع التهديد؛ فالذكاء الاصطناعي يوفر فرصة للانتقال نحو (الأمن التنبؤي) الذي يستشرف الأزمات قبل حدوثها عبر تحليل البيانات الضخمة، وهو ما يمثل "الرافعة الاستراتيجية" المطلوبة للمنظومة العربية.

بناءً على ذلك، يمكن أن نوصي بالآتي:

1. تأسيس منصة عربية موحدة لتبادل الاستخبارات الرقمية، لتأمين القدرة على الإنذار المبكر واللحظي ضد الجيوش السيبرانية العابرة للحدود.

2. إنفاذ السيادة التشريعية لتوطين البيانات (Data Localization)، عبر قوانين إلزامية تجبر الاحتكارات التكنولوجية العالمية على تخزين البيانات الحساسة داخل الحدود الجغرافية، بالتزامن مع بناء حوسبة سحابية عربية مشتركة عِبر مراكز بيانات عملاقة مستقلة تقلل الاعتماد على البرمجيات المستوردة

3. الاستثمار في أنظمة الدفاع الذاتي (Self-healing systems) لحماية البنى التحتية الحيوية (كالطاقة والأنظمة المالية) آلياً وتجنب سيناريو الشلل الوطني البنيوي.

4. إنشاء معاهد بحثية عسكرية متخصصة في الذكاء الاصطناعي، لتأهيل جيل من المحللين الاستراتيجيين القادرين على إدارة الحروب الخوارزمية ومنع هجرة العقول.

Conclusion:

Resilience in the digital age is not merely a technological arms race; it is a conflict of wills to possess the algorithms that will govern the balance of power in the new international order. True national sovereignty will only be achieved when the Arab security mindset shifts from a state of "reaction" to a state of "digital leadership."

The future of Arab security in the age of AI is contingent upon the ability to transition from technical consumption to knowledge-based and sovereign production. The upcoming battle is not on the ground, but rather a battle over the algorithm. Those who possess the capability to direct AI will shape the future of sovereignty, while those absent from this field will find themselves in a state of permanent digital dependency.

In light of this, the key conclusions can be summarized as follows:

1. The Limitations of Classical Deterrence: Traditional deterrence systems now suffer from a "response deficit" against automated attacks and drone swarms managed by algorithms that exceed the speed of human perception.
2. The Risk of Closed-Source Dependency: Relying on foreign security systems (closed-source code) represents a strategic vulnerability. These imported technologies could act as "double agents" during crises, making reverse engineering and the localization of software a paramount security necessity.
3. Cyberspace as the Fifth Domain: The crystallization of the digital realm as a fifth sovereign domain requires unified Arab legal and legislative governance to bridge the regulatory gap currently exploited by armed groups and non-state actors.
4. The Shift to Predictive Security: It is no longer enough to wait for a threat to materialize. Artificial Intelligence provides an opportunity to transition toward "Predictive Security," which anticipates crises before they occur through Big Data analysis. This represents the "strategic lever" required for the Arab security framework.

Based on this, the following is recommended:

1. Establishing a unified Arab platform for exchanging digital intelligence to ensure early and real-time warning capabilities against transnational cyber armies.
2. Enforcing legislative sovereignty for data localization through mandatory laws that compel global technology monopolies to store sensitive data within Arab geographic borders, while simultaneously building a shared Arab cloud computing infrastructure through independent mega data centers that reduce reliance on imported software.
3. Investing in self-healing systems to automatically protect critical infrastructure (such as energy and financial systems) and prevent structural national paralysis.
4. Establishing specialized military research institutes in artificial intelligence to train a generation of strategic analysts capable of managing algorithmic warfare and preventing brain drain.

المصادر :

- أوسوبا، اوسوندي أ. ووليام ويلسر الرابع. مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل (مؤسسة RAND ٢٠١٧).
- رضا، فادي علي. الهندسة العكسيّة للذكاء الاصطناعي في الحروب الحديثة: مقاربة سوسيولوجيّة عسكريّة، **مجلة أوراق ثقافية**، العدد ٣٨ (دار الأمير للثقافة والعلوم، لبنان: ٢٠٢٥/٧/١٦).
- الرميحي، محمد. **الأمن القومي العربي في عصر الرقمنة: التحديات والفرص** (مركز دراسات الوحدة العربية، بيروت: 2024).
- زيتون، محمد محمود. "العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني"، **المجلة العربية للنشر العلمي**، العدد٧٧، (منظمة المجتمع العلمي العربي، قطر: ٢ آذار ٢٠٢٥).
- السعبري، بهاء عدنان. وعماد عبد خضير الزرفي، "العناصر التقنية للتهديد الالكتروني"، **مجلة مركز دراسات الكوفة**، العدد ٥٧، (النجف: ٣٠ حزيران ٢٠٢٠).
- العبيدي، ليث عصام مجيد، "الذكاء الاصطناعي والوجود الإنساني: قراءة فكرية في الابعاد العسكرية"، **المجلة السياسية الدولية**، العدد ٥٨، (الجامعة المستنصرية: ١ اذار ٢٠٢٤).
- العتيبي، منيرة. "الذكاء الاصطناعي في الشؤون العسكرية: تحولات العقيدة والردع"، **(مركز الملك فيصل للبحوث والدراسات الإسلامية**، الرياض: 2023).
- عمر، ايمن. "أثر التكنولوجيا على نظريات الجغرافيا السياسية (الفضاء السيبراني باعتباره إقليم جديد)"، **دراسات بحثية**، (المركز الديمقراطي العربي، ألمانيا: ١٨ تموز ٢٠٢٥).
- عرض كتاب: (فرجاني، علي. **"التزييف العميق وتقنيات الخداع الرقمي – دراسة متعمقة في التحديات المهنية والتقنية**، دار السحاب للنشر والتوزيع: القاهرة، ٢٠٢٤)، في: **مجلة اتجاهات سياسية**، المجلد (٨)، العدد (٢٩)، (المركز الديمقراطي العربي، ألمانيا: كانون الأول ٢٠٢٤).
- غركان، عمار مراد. "التعاون الدولي للتصدي لخطر الإرهاب باستخدام الذكاء الاصطناعي، مستقبل الذكاء الاصطناعي: تحديات قانونية واخلاقية"، **مجلة قضايا التطرف والجماعات المسلحة**، المجلد ٦ العدد ١٧ (المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا: تشرين الثاني ٢٠٢٤).
- الفرساوي، عبد القادر. "الحروب الهجينة والرمادية وعلاقتها بالجماعات الإرهابية" **مجلة قضايا التطرف والجماعات المسلحة**، المجلد ٦ العدد ٢٠ (المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا: آب ٢٠٢٥).
- محمد، حسن علي. "ثلاثية الاستعمار الرقمي، **مجلة بحوث الإعلام الرقمي**"، العدد (١٠)، (جامعة السويس، كلية الاعلام وتكنولوجيا الاتصال: كانون الثاني/ أذار ٢٠٢٦).
- المنظمة العربية لتكنولوجيات الاتصال والمعلومات، **"الاستراتيجية العربية للأمن السيبراني٢٠٢٣-٢٠٢٧"**، (جامعة الدول العربية، تونس: ٢٠٢٣).
- المنظمة العربية لتكنولوجيات الاتصال والمعلومات، **"الرؤية العربية للأمن السيبراني: الواقع – التحديات – الفرص"**، (جامعة الدول العربية، تونس: ٢٠٢١).
- اسلام عبد المجيد عيد، الحرب الهجينة: صورة أخرى للصراع في الشرق الأوسط ما بعد عام ٢٠١١، منصة الجيوسياسية، ٢٠٢١/٣/٢٨، https://www.wgi.world/alharb-alhajinat-surat-ukhraa-lilsirae-fi-alshr-al-awsat-2011ma-/?lang=ar

- بن ناصر، ناصر. "أثر الذكاء الاصطناعي على الأمن الإقليمي وتصورات الهديدات، ومبادرة انشاء منطقة الشرق الأوسط كمنطقة خالية من أسلحة الدمار الشامل"، (معهد الأمم المتحدة لبحوث نزع السلاح: ٢٠٢٥).https://unidir.org/wp-content/uploads/2025/02_Impact_of_Artificial_Intelligence_on_Regional_Security_UNIDIR_AR.pdf

- مركز الإمارات للدراسات والبحوث الاستراتيجية. تعزيز ركائز الدولة الوطنية في الشرق الأوسط: الإشكاليات الراهنة والاستراتيجيات المقترحة، تمت الزيارة بتاريخ ٢٠٢٦/٣/٣.https://www.ecssr.ae/ar/research-products/periodic-studies-3/1/203833

- نبيل فهمي، نحو منظومة أمنية عربية وشرق أوسطية، جريدة الشروق، مصر، ١٦ أذار ٢٠٢٦.https://www.shorouknews.com/columns/view.aspx?cdate=16032026&id=6722429-4461f-e26d4-aaaa-3850-5636-84357

- هيثم جبار طه، "التحديات الأمنية التي تواجه الدول العربية في مجال السيادة الرقمية"، وكالة الحدث الإخبارية، ٥ آب ٢٠٢٥.https://www.alhadathcenter.net/index.php/views/145576-2025-08-05-14-55-23

Reference:

- Héau, Lauriane. and Giovanna Maletta, "Arms Transfer and SALW Controls in the Middle East and North Africa: Challenges and State of Play.", Stockholm International Peace Research Institute, 1 November 2022, https://www.sipri.org/commentary/topical-backgrounder/2022/arms-transfer-and-salw-controls-middle-east-and-north-africa-challenges-and-state-play
- Johnson, James. "Artificial Intelligence and the Future of Warfare: The USA, China, and Strategic Stability." (Oxford University Press: 2021).
- Martin. Lockheed, "Layered Defense, Orbital Advantage: The Space Domain's Rising Role." 11 Aug. 2025, https://www.lockheedmartin.com/en-us/news/features/2025/layered-defense-orbital-advantage-the-space-domains-rising-role.html
- NATO, "NATO Integrated Air and Missile Defence Policy." 13 Feb. 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-integrated-air-and-missile-defence-policy
- NAUSS & UNICRI, "1st Artificial Intelligence Forum for Law Enforcement Uses." (Naif Arab University for Security Sciences: 4-5 October 2023).
- Nye, Joseph S. "Power in the Cyber Age." (Oxford University Press: 2017).
- Payne, Kenneth. "Warbot: The Dawn of Artificially Intelligent Conflict." (Hurst & Company, London: 2021).
- Sanaullah Khan, Muhammad. Farhat Asghar Rana, Zoha Irfan, "Hybrid Warfare in the Digital Age: Cyberpower, AI, and the future global security." Advance Social Science Archive Journal, Vol.04 No. 01 (July-September 2025).
- Scharre, Paul. "Four Battlegrounds: Power in the Age of Artificial Intelligence." (W. W. Norton & Company, New York: 2023).
- Schwab, Klaus. "Shaping the Future of the Fourth Industrial Revolution." (World Economic Forum, 2018).
- Shaman, Aleksandr. "AI's invisible invasion: how artificial intelligence is becoming the newest weapon in hybrid warfare." ESCP international politics society, (21 July 2025).
- Wanigathunga, Vimukthi. "Reverse Engineering & How it approach into cyber Security" Research Gate: November 2020).
- World economic forum, "The global risks report." 11 January 2023. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf