Journal of Al-Farahidi's Arts, No Conference (10 th)N(III)103-122
Doi: https://doi.org/10.25130/jfa.conf.10.3.7

Proceedings of the (10) Conference وقائع المؤتمر العلمي العاشر

P-ISSN : 2074-9554 | E-ISSN: 2663-811
Journal of Al-Farahidi's Arts
available online at : fja.tu.edu.iq/index.php/fja

Tikrit University J.F.A Journal of Al-Frahedis

The Use of Artificial Intelligence in the Russian-Ukrainian War of 2014-2025 A Historical Study

M.M. Hawazen Saad Ihsan Al-Douri
M.M. Tariq Hamed Majbal Al-Issawi

E-Mail: taraq.hamed1996@gmail.com

Keywords:
Russia, Ukraine, artificial intelligence,
he Russian-Ukrainian war

Article history:

Received	25/7/2025
Received in revised form	7/8/2025
Accepted	19/10/2025
Available online	9/12/2025

E-mail Jaa@ tu.edu.iq

©THIS AN OPEN ACCESS ARTICLE UNDER THE CCBY LICENSE
http:// creativecommons.org/licenses/by/4.0

A B S T R A C T

The Russia-Ukraine conflict has accelerated the use and development of artificial intelligence in the military arena. Russia has used it in drones, cyberattacks, and communications disruption, giving it an advantage in executing precise and rapid attacks. This conflict serves as a laboratory for testing military AI capabilities among major powers. AI has also influenced international politics through cyberwarfare, autonomous weapons, and disinformation campaigns. It has contributed to improved information gathering and analysis, supported negotiations between Russia and Ukraine, and influenced public diplomacy by changing propaganda methods on social media.

توظيف الذكاء الاصطناعي في الحرب الروسية الاوكرانية عام ٢٠١٤-٢٠٢٥

دراسة تأريخية

م. طارق حامد مجبل العيساوي /جامعة الانبار / كلية التربية للعلوم الإنسانية
م.م هوازن سعد احسان الدوري

المستخلص:

الصراع الروسي الأوكراني أدى إلى تسريع استخدام وتطوير الذكاء الاصطناعي في المجال العسكري، حيث استخدمته روسيا في الطائرات المسيرة، الهجمات الإلكترونية، وتعطيل الاتصالات، مما منحها ميزة في تنفيذ هجمات دقيقة وسريعة. ويُعد هذا الصراع بمثابة مختبر لاختبار قدرات الذكاء الاصطناعي العسكرية بين القوى الكبرى. كما أثّر الذكاء الاصطناعي في السياسة الدولية من خلال الحرب السيبرانية، الأسلحة ذاتية التشغيل، وحملات التضليل، وساهم في تحسين جمع المعلومات والتحليلات، ودعم التفاوض بين روسيا وأوكرانيا، بالإضافة إلى تأثيره في الدبلوماسية العامة من خلال تغيير أساليب الدعاية عبر وسائل التواصل الاجتماعي.

الكلمات المفتاحية : روسيا، أوكرانيا، الذكاء الاصطناعي، الحرب الروسية الأوكرانية

المقدمة:

تُعدّ الحرب الروسية الأوكرانية مثالاً بارزًا يُجسّد الطبيعة الديناميكية والمرنة للتهديدات السيبرانية، وقد تمثّل ذلك في استهداف البنية التحتية الرقمية، وتوظيف قدرات استخباراتية متطورة لاختراق قواعد البيانات وزرع البرمجيات الخبيثة، بهدف تعطيل مؤسسات الدولة المختلفة على الصعد الإدارية، الصحية، التعليمية، وقطاع الطاقة. وقد أصبح الذكاء الاصطناعي أداةً متزايدة الأهمية في الحروب الحديثة، إذ يوفر قدرات هجومية ودفاعية للجيوش في جميع أنحاء العالم. ومع ذلك، يثير استخدام الذكاء الاصطناعي في الحروب تساؤلات أخلاقية وقانونية معقدة، لا سيما في سياق أنظمة الأسلحة ذاتية التشغيل. أثار الصراع الروسي الأوكراني مخاوف بشأن استخدام الذكاء الاصطناعي لأغراض عسكرية، بما في ذلك تسليحه، حيث استخدم كلا الجانبين أسلحةً تعمل بالذكاء الاصطناعي، مثل الطائرات المسيرة والمركبات ذاتية القيادة، والهجمات السيبرانية، لإجراء عمليات بدقة وكفاءة أكبر.

وقد قسم البحث الى مقدمة واربع مباحث وخاتمة وقائمة بالمصادر، تطرق المبحث الأول الى أسباب الحرب ومجرياتها، تناول المبحث الثاني الذكاء الاصطناعي في الحروب، اما المبحث الثالث فقد تطرق الى استخدام روسيا وأوكرانيا الطائرات بدون طيار في الحرب، في حين تحدث المبحث الرابع عن الهجمات السيبرانية في الحرب الروسية الأوكرانية.

المبحث ألاول: أسباب الحرب

ترجع بدايات الأزمة الأوكرانية إلى الاحتجاجات التي اندلعت ضد الرئيس فيكتور بانوكوفيتش عقب توقيعه اتفاقًا مع موسكو يقضي بمنح أوكرانيا مساعدات مالية بقيمة 51 مليار دولار، إضافة إلى خفض سعر الغاز إلى ما يقارب الثلث، وهو سعر تفضيلي غالبًا ما تقدمه روسيا للدول التي كانت ضمن الاتحاد السوفيتي وتعتبرها شريكة استراتيجية (عبد الغني ، 2013 ، ص2).

أن جذور الأزمة تعود إلى ما هو أعمق، حيث اندلعت في 21 تشرين الثاني 2004 ما عُرف بـــ"الثورة البرتقالية"(**اندلعت الثورة البرتقالية في أوكرانيا أواخر تشرين الثاني 2004 واستمرت حتى كانون الثاني 2005، واتخذت من الوشاح البرتقالي رمزًا لها، وهو رمز يُعبّر عن الطابع السلمي للثورات. جاءت هذه الحركة على خلفية احتجاجات واسعة**

وأحداث سياسية متلاحقة، نتيجة اتهامات بتزوير الانتخابات الرئاسية. وقد نظّمت المعارضة مظاهرات جماهيرية كبيرة رفضًا لنتائج الانتخابات، ما دفع المحكمة العليا إلى الاعتراف بوقوع التزوير، وإلغاء النتائج المعلنة، والدعوة إلى إعادة الاقتراع في كانون الاول 2004. وأسفرت جولة الإعادة عن فوز مرشح المعارضة فيكتور يوشينكو، الذي تسلّم السلطة لاحقًا . ينظر: ياس، ص٨٧) نتيجة اتهامات بتزوير الانتخابات الرئاسية آنذاك. فقد اتُّهم نظام الرئيس ليونيد كوتشما بمحاولة إيصال مرشحه الموالي لروسيا، فيكتور يانوكوفيتش، إلى سدة الحكم على حساب مرشح المعارضة المدعوم من الغرب، فيكتور يوشينكو، مما دفع المعارضة إلى الدعوة للتظاهر احتجاجًا على نتائج الانتخابات (عبد الغني ، ٢٠١٣، ص٢).

تصاعد التوتر السياسي في أوكرانيا، وازداد الانقسام داخل البرلمان، حيث انقسم أعضاؤه بين مؤيدين لروسيا الاتحادية وآخرين داعمين للتوجه الغربي. ومع فوز الكتلة المؤيدة للغرب، تفاقمت الأزمة في أوائل عام 2009، لاسيما بعد أن قررت روسيا رفع أسعار الغاز الطبيعي ووقف إمداداته إلى أوكرانيا. جاء ذلك في وقت كانت فيه البلاد تعاني من تداعيات الأزمة المالية العالمية، مما كشف بوضوح مدى التأثير العميق الذي تستطيع روسيا ممارسته على الداخل الأوكراني (الشرقاوي ، ٢٠٠٩، ص١٠٠).

أدركت أوكرانيا أهمية روسيا كمصدر حيوي لإمدادات الطاقة، وقد شكّلت الانتخابات الرئاسية عام 2010 نقطة تحول بارزة، حيث أسفرت نتائجها عن فوز فيكتور يانوكوفيتش في الجولة الأخيرة، وهو ما اعتُبر انتصارًا لروسيا وحلفائها داخل أوكرانيا. هذا الفوز مثّل انعطافة في مسار العلاقات بين البلدين، إذ أعاد الدفء والتقارب إلى العلاقات الثنائية، كما أُعيد اعتماد اللغة الروسية كلغة رسمية في البلاد (عبد العاطي ، ٢٠١٠، ص ٢٠٣).

تجددت الأزمة الأوكرانية في كانون الاول 2013 عقب اندلاع موجة من الاحتجاجات الشعبية، وذلك على خلفية قرار الرئيس فيكتور يانوكوفيتش رفض توقيع اتفاقية الشراكة والتجارة الحرة مع الاتحاد الأوروبي، ما أثار غضب مؤيدي التوجه الأوروبي وأشعل فتيل التوتر في البلاد من جديد (أسامة، ٢٠١٤، ص ١). وشكّلت العلاقة مع الاتحاد الأوروبي العامل الأساسي وراء الأزمة الأوكرانية واندلاع موجة الاحتجاجات المعروفة بالانتفاضة الأوكرانية الثانية، التي وقعت خلال أقل من عقد من الزمن. وتجدر الإشارة إلى أن هذه العلاقة لم تكن مجرد خيار سياسي، بل عكست سلسلة من التحديات الاستراتيجية والاقتصادية

والسياسية التي تواجهها أوكرانيا كجزء من سعيها لترسيخ هويتها كدولة مستقلة ونظرًا للترابط الوثيق بين استقرار أوكرانيا وأمن إمدادات الطاقة إلى أوروبا، بادر الاتحاد الأوروبي إلى فتح مفاوضات مع كييف بشأن إبرام اتفاق شراكة مميزة. وقد أسفرت هذه المفاوضات عن عرض قدّمه الاتحاد للرئيس يانوكوفيتش في تشرين الثاني، لكنه اعتبره غير كافٍ لتلبية الحاجات المالية العاجلة للبلاد. وبينما كان لا يزال يدرس القرار، فوجئ يانوكوفيتش بخروج حشود من المواطنين إلى ميدان الاستقلال في كييف، مطالبين بتوقيع الاتفاق والضغط عليه للانضمام إلى الشراكة الأوروبية (نافع ، ٢٠١٤، ص٣).

عقب رفض العرض الأوروبي، تقدّم الرئيس الروسي فلاديمير بوتين بعرض مغرٍ لأوكرانيا، تضمن حزمة مساعدات مالية بقيمة 51 مليار دولار إلى جانب تخفيض كبير في أسعار الغاز. وقد رأى بوتين في هذا العرض وسيلة فعالة لإبعاد أوكرانيا عن دائرة النفوذ الأوروبي، بينما اعتقد يانوكوفيتش أن هذه الخطوة ستكون كفيلة بتهدئة الشارع ووقف موجة الاحتجاجات المتصاعدة (نافع، ٢٠١٤، ص ٤)

بدأ البرلمان الأوكراني، الذي شهد تحولًا في موازين القوى من الحزب الحاكم إلى المعارضة، باتخاذ خطوات لتنفيذ مطالب الشارع واحتواء الأزمة، في محاولة لتفادي الانزلاق نحو حرب أهلية. فقد تم إقالة حكومة يانوكوفيتش، وأُعيد العمل بدستور عام 2004 الذي يقيد صلاحيات الرئيس ويعزز سلطات البرلمان. كما صوتت غالبية النواب على عزل يانوكوفيتش من منصبه، الأمر الذي دفعه إلى مغادرة القصر الرئاسي والتوجه نحو شرق البلاد، بعد فشل محاولته مغادرة أوكرانيا عبر طائرة خاصة. وعلى الرغم من رفضه لقرار البرلمان بإقالته، فإن مهام رئيس الجمهورية كانت قد أُسندت رسميًا إلى رئيس البرلمان بتصويت الأغلبية(نافع، ٢٠١٤، ص ٥). من جهتها، استغلت روسيا حالة الفوضى التي عمّت أوكرانيا لتتدخل عسكريًا في شبه جزيرة القرم، مبررة ذلك بضرورة حماية المواطنين من أصول روسية. إذ تضم المناطق الشرقية من أوكرانيا، بما في ذلك القرم، نسبة كبيرة من السكان ذوي القومية الروسية. وقد أثار هذا التدخل ردود فعل غاضبة من الولايات المتحدة والدول الأوروبية، التي اعتبرته انتهاكًا للسيادة الأوكرانية وتصعيدًا خطيرًا في الأزمة (راشد، ٢٠١٤، ص ١٢٢).

وقد أدانت الولايات المتحدة الأمريكية والدول الأوروبية قيام روسيا بضم شبه جزيرة القرم، كما رفضت الحكومة الأوكرانية هذا الإجراء، مؤكدة أن انضمام القرم إلى روسيا تم

دون موافقة السلطة المركزية في كييف. واعتبرت أوكرانيا والمجتمع الدولي أن ما حدث يُعد انتهاكًا واضحًا للقانون الدولي، الذي يشترط الحصول على موافقة الحكومة المركزية قبل إجراء أي استفتاء يفضي إلى تغيير في السيادة (راشد، ٢٠١٤،ص ١٢٧). وقد عكس ضم موسكو الجزيرة القرم تأمين قواعد أسطول البحر الأسود أكثر من حماية المواطنين الروس (Richter 2022.p3).

المبحث الثاني: الذكاء الاصطناعي في الحروب

يُعد توظيف الذكاء الاصطناعي في الأنظمة التسليحية مجالًا ناشئًا يثير جدلاً واسعًا في الأوساط الأكاديمية والعسكرية، لاسيما فيما يتعلق بالأسلحة ذاتية التشغيل القادرة على اتخاذ قرارات وتنفيذ إجراءات قتالية دون تدخل بشري مباشر. وتُثير هذه الأنظمة مخاوف جدية بشأن إمكانية التسبب في أضرار غير مقصودة، وصعوبة التحكم بها في بيئات القتال المعقدة. وقد اظهر الصراع الروسي–الأوكراني هذا التوجه بشكل واضح، حيث أفادت تقارير موثوقة بأن روسيا قد لجأت إلى نشر أنظمة تسليحية تعتمد على الذكاء الاصطناعي، مما يسلّط الضوء على التحول المتسارع في طبيعة الحرب الحديثة ودور القرارات الذاتية في ساحة المعركة (Ivan, 2024, 1).

حيث قد تُخطئ هذه الأنظمة في تفسير البيانات أو تحديد الأهداف، ما يؤدي إلى استهداف المدنيين أو إلحاق أضرار جسيمة بالبنية التحتية الحيوية. ويُفاقم هذا الخطر **غياب الرقابة البشرية المباشرة**، إذ لا تتوفر آلية تدخل فوري لتصحيح الأخطاء أو إيقاف العمليات في حال حدوث خلل، مما يُثير تساؤلات أخلاقية وقانونية حول مدى موثوقية هذه الأنظمة ومسؤولية استخدامها في النزاعات المسلحة (Scharre, 2018,20).

من بين المخاوف الجوهرية المرتبطة بالأسلحة ذاتية التشغيل **صعوبة التحكم والسيطرة بعد تفعيلها**، إذ قد تُواجه الجيوش تحديات تقنية وأمنية في استدعاء هذه الأنظمة أو إيقاف تشغيلها بمجرد دخولها حيز التنفيذ، إذ يمكن أن تستمر هذه الأسلحة في تنفيذ عمليات هجومية حتى بعد زوال الحاجة إليها، أو تُستخدم بشكل غير مقصود نتيجة خلل في البرمجة أو التفاعل غير المتوقع مع البيئة التشغيلية. وتُعد هذه الإشكالية من أبرز التحديات في ضمان الاستخدام الآمن والمسؤول للذكاء الاصطناعي في السياقات العسكرية (Arkin, 2015, 25).

المبحث الثالث: استخدام الطائرات بدون طيار في الحرب الروسية الاوكرانية

تعود بدايات تطوير تقنيات الطائرات بدون طيار إلى أوائل القرن العشرين، استنادًا إلى مفهوم التحكم بالمركبات الجوية عن بُعد دون تدخل بشري مباشر. وقد شقّت هذه التقنية طريقها إلى الاستخدامات العسكرية لأول مرة خلال الحرب العالمية الأولى، حيث برزت طائرة "كيترينج بَج" (Kettering Bug)، التي طوّرها المهندس تشارلز فرانكلين كترنج (Charles F. Kettering)عام 1917، بوصفها أحد أوائل النماذج العملية للطائرات ذاتية التوجيه المُصممة لأغراض هجومية (Rusya–Ukrayna, 2025,p 14).

كما شكّلت قنابل V–1 الألمانية الطائرة خلال الحرب العالمية الثانية دليلاً مبكراً على الإمكانات الاستراتيجية للطائرات بدون طيار في السياقات العسكرية، وذلك بمدى يصل إلى 250 كيلومترًا وقدرة تدميرية عالية عند بلوغ الهدف، مثّلت هذه القنابل نقلة نوعية في استخدام المركبات الجوية ذاتية التوجيه، حيث ركزت تقنياتها آنذاك على تحسين أنظمة التوجيه والقدرة على حمل المتفجرات بفعالية(Hamad & Alaiwi, 2022, p. 1–6) .

شهدت فترة الحرب الباردة توسعًا ملحوظًا في استخدام تكنولوجيا الطائرات بدون طيار لأغراض الاستطلاع والاستخبارات، لاسيما من قبل الولايات المتحدة خلال ستينيات القرن العشرين. وقد مثّلت الطائرة المسيرة "ريان فايربي" (Ryan Firebee) نموذجًا رائدًا في هذا المجال، حيث استُخدمت في مهام التصوير وجمع المعلومات الاستخبارية، مع تعزيز قدراتها التشغيلية لتلبية متطلبات البيئة العسكرية آنذاك (Hall, 2014, p.20–27).

شهدت التسعينيات تحولاً جوهرياً في تكنولوجيا الطائرات بدون طيار، حيث استخدمت الولايات المتحدة طائرات Pioneer RQ–2 خلال حرب الخليج الثانية للكشف عن الأهداف وتوجيه نيران المدفعية (Stracker, Matthew, 2007, p.8)، مما أحدث نقلة نوعية في ديناميكيات العمليات العسكرية بفضل المعلومات الاستخباراتية الفورية. وساهم تطور تقنيات GPS والاتصالات الرقمية في تعزيز دقة وكفاءة هذه الطائرات. وفي عام 1999، استخدم حلف الناتو طائرات Predator RQ–1 في حرب كوسوفو لأغراض المراقبة وجمع المعلومات، وبرزت كأول طائرة بدون طيار حديثة تجمع بين مهام الاستطلاع والقدرات الهجومية. ومع بداية الألفينيات، أصبحت الطائرات بدون طيار عنصراً فاعلاً في النزاعات المسلحة، حيث سلّحت الولايات المتحدة طائرات Predator في عام 2001 لاستهداف

عناصر القاعدة في أفغانستان، وتم تطوير Predator MQ-1 المزودة بصواريخ Hellfire لتنفيذ ضربات دقيقة، مما شكل نقطة تحول نحو الاستخدام القتالي المنهجي للطائرات بدون طيار (Rusya-Ukrayna, 2025,p 15).

وفي العقد الأول من القرن الحادي والعشرين شهد تطورًا ملحوظًا في فعالية الطائرات بدون طيار، أذ استخدمت الولايات المتحدة طائرات Reaper MQ-9 ذات الحمولة البالغة 1701 كجم في عمليات استخبارية وهجومية في مناطق مثل أفغانستان والعراق (Youvan, 2024 , p.2). وتميزت تلك الطائرات بقدرتها على تنفيذ ضربات دقيقة وجمع معلومات استخبارية عالية القيمة، إلى جانب استخدامها في مهام أمن الحدود. وفي الوقت ذاته، ظهرت الصين كفاعل رئيسي في هذا المجال، أذ طورت نماذج مثل Wing Loong و CH-4، التي حظيت بإقبال دولي بفضل تكلفتها المنخفضة وكفاءتها التشغيلية. وأسهمت تلك الاختراقات التكنولوجية في تعزيز دور الطائرات بدون طيار ضمن الاستراتيجيات العسكرية العالمية (Pettyjohn, Dennis& Campbell, 2024, p.14)

ظهرت تركيا كأحد الفاعلين الرئيسيين في مجال الطائرات بدون طيار خلال العقدين الأول والثاني من القرن الحادي والعشرين، حيث تسارعت جهودها في تطوير منصات محلية مثل Bayraktar TB2 وANKA (Çetinkaya, & Koç, 2023, p.1-27). وقد لعبت هذه الأنظمة دورًا محوريًا في عمليات مكافحة الإرهاب وأمن الحدود، وبرزت فعاليتها خلال عملية درع الفرات عام 2016 (Ateş, 2021, p. 7-16). وفرّت هذه الطائرات قدرات متقدمة في الاستطلاع والهجوم، وأسهمت في تعزيز الكفاءة العملياتية. واعتماد تركيا على الإنتاج المحلي قلل من تبعيتها للخارج، وجعلها مصدرًا عالميًا لتقنيات الطائرات بدون طيار (Kinik & Çelik, 2021, p.174).

تمثل عشرينيات القرن الحادي والعشرين حقبة مفصلية في تطور استخدام الطائرات بدون طيار في ميادين القتال، أذ ظهرت بشكل لافت خلال الحرب الروسية-الأوكرانية. فقد أظهرت تلك الحرب الاستخدام الواسع والمبتكر لتقنيات الطائرات بدون طيار، إذ قامت أوكرانيا بتعديل طائرات تجارية بدون طيار، مثل طائرات DJI Phantom، وتوظيفها في مهام استطلاعية وأخرى هجومية، بما في ذلك تنفيذ هجمات انتحارية. في المقابل، اعتمدت روسيا بشكل مكثف على الطائرات الإيرانية الصنع من طراز Shahed-136 (Sharma,

2025, p.900) ، إلى جانب استخدامها طائرات روسية مثل Orlan-10 وLancet-3 التي أثبتت فعاليتها في عمليات المراقبة والهجوم (Eslami, 2022, p. 507-518).

أخذ النزاع الروسي الأوكراني تحولًا نوعيًا في طبيعة الحروب الحديثة، أذ وُصفت بأنها أول "حرب طائرات بدون طيار ورقمية وسيبرانية" في التاريخ العسكري. على خلاف الحروب السابقة التي اتسم فيها استخدام الطائرات المسيّرة بطرف واحد، اعتمد الطرفان في هذا الصراع بشكل نشط على طائرات بدون طيار محلية وأجنبية (Rusya-Ukrayna, 2025,p 24).

بدأ تطوير الطائرات بدون طيار في الحقبة السوفيتية بنماذج رائدة مثل **Tu-141 Strizh** و**Tu-143 Reis**، التي دخلت الخدمة في السبعينيات لأغراض الاستطلاع. وفي الثمانينيات، أصبحت جزءًا من عقيدة "مجمع الاستطلاع الهجومي"، لاسيما في دعم وحدات المدفعية. غير أن تلك الجهود شهدت تراجعًا كبيرًا بعد انهيار الاتحاد السوفيتي، ما أدى إلى تباطؤ التطور التكنولوجي في هذا المجال خلال تسعينيات القرن الماضي (Luzin, 2024, p. 2).

وفي أواخر العقد الأول من القرن الحادي والعشرين، عززت روسيا جهودها لتطوير أنظمة الطائرات بدون طيار من خلال إشراك شركات خاصة وأخرى مدعومة من الدولة، مثل مجموعة "زالا آيرو" و"كرونشتات"، في مشاريع تهدف إلى رفع قدراتها في هذا المجال. ومع ذلك، لم تحقق النماذج التي طُوّرت خلال تلك الفترة سوى نجاح تشغيلي محدود نتيجة تحديات فنية وتقنية. وفي السنوات الأخيرة، كثّفت روسيا استثماراتها في تكنولوجيا الطائرات غير المأهولة عبر نماذج متقدمة، منها أورلان-10، وفوربوست، وألتيوس، وإس-70 أوخوتنيك. ويُعد نظام أورلان-10 أحد أبرز هذه النماذج، أذ صُمم لأغراض الاستطلاع التكتيكي، ويتميّز بإمكانية دمجه مع أنظمة الحرب الإلكترونية لأداء مهام متعددة في بيئات عمليات معقدة (https://www.lrt.lt/en/news-in-english).

يواجه برنامج الطائرات المسيرة الروسي تحديات هيكلية تتعلق بإنتاج المحركات وتوفير المكونات الإلكترونية، إذ تعاني محركات محلية مثل **VK-800SM**، المخصصة لطائرة **Altius**، من مشكلات في الإنتاج والتصدير. ويحد هذا الواقع من قدرة روسيا على التحديث والإنتاج الواسع. لا تزال معظم المسيّرات الروسية تعتمد على مكونات مستوردة،

وقد تفاقم هذا الاعتماد بفعل العقوبات الدولية منذ عام 2022. وعلى الرغم من اللجوء إلى بدائل منخفضة التكلفة من الصين ودول أخرى. كما يُبرز الاستخدام الواسع للطائرتين الإيرانيتين Shahid-131 و Shahid-136 ضعف الإنتاج المحلي واعتماد روسيا المتزايد على الموردين الخارجيين(Bilousova, Zagrebelska, Vlasiuk, & Shapoval, 2023, p. 4-7)

تُعد الطائرة الإيرانية Shahid-131 خيارًا مفضلًا للعمليات منخفضة الكلفة نظرًا لحجمها الصغير وبساطة تصميمها، وقد تم رصد استخدامها لأول مرة في أوكرانيا خلال خريف عام 2022. في المقابل، تتميز Shahid-136 بهيكل ومحرك أكبر، ما يجعلها أكثر ملاءمة للهجمات بعيدة المدى. ويُظهر تصميمها، خاصة الجناح المثلثي والمحرك الخلفي، توازنًا عاليًا بين الكفاءة التشغيلية والتكلفة المنخفضة. وقد أثبتت تلك الأنظمة، ولا سيما "شهيد-136"، فاعليتها في استهداف البنية التحتية الحيوية للطاقة والمنشآت المدنية في أوكرانيا، ما يعكس تأثيرها المدمر ودورها المتزايد في العمليات العسكرية (Iranian UAVs) .in Ukraine, 2023, p.4-7

يعكس هذا الوضع اعتماد روسيا الكبير على مصادر خارجية لتأمين المكونات الاستراتيجية اللازمة لتكنولوجيا الطائرات المسيرة، مما يظهر محدودية قدراتها الإنتاجية المحلية في مجال التكنولوجيا المتقدمة. وتشير تحليلات سلاسل التوريد المستندة إلى بيانات التجارة العالمية إلى أن الصين تُعد المورّد الرئيسي، حيث توفر نحو 67% من هذه المكونات، في حين تُنقل 17% إضافية عبر هونغ كونغ. وخلال النصف الأول من عام 2023، بلغ حجم تجارة تلك المكونات 7.2 مليار دولار أمريكي، مسجلًا زيادة بنسبة 19% مقارنة بالفترة نفسها من العام السابق، ما يؤكد استمرار اعتماد روسيا على الإمدادات الأجنبية لتعويض فجواتها الصناعية والتكنولوجية (Rusya-Ukrayna, 2025,p 34).

كان للتطورات في أوكرانيا تداعيات دبلوماسية واسعة النطاق، إذ دفعت العديد من الدول إلى إعادة تقييم استراتيجياتها الدفاعية في ضوء الدور المتزايد لتكنولوجيا الطائرات بدون طيار. وقد اختارت دول عدة، ولا سيما في الغرب، زيادة استثماراتها في هذا المجال وفي التدابير المضادة ذات الصلة (Sharma, 2025, p. 908-909) كما عززت الدول الغربية دعمها لأوكرانيا من خلال تزويدها بطائرات مسيّرة ومعدات استخباراتية متقدمة، ما

كرّس أهمية الابتكار التكنولوجي في الحفاظ على توازن القوى الدولي. ولم يقتصر تصاعد الدعم العسكري على تحقيق مكاسب تكتيكية لأوكرانيا، بل عكس أيضًا تحولًا أوسع في أولويات السياسات الدفاعية العالمية نحو الاعتماد المتزايد على الأنظمة غير المأهولة والآلية (Favaro & Williams, 2023, p.30–35).

خلال مدة الحرب، شهدت القدرة الإنتاجية العسكرية لأوكرانيا تطورًا ملحوظًا، يعكس تنامي الاعتماد على القدرات الذاتية في تلبية احتياجات الدفاع الوطني. ويعمل في قطاع الصناعات الدفاعية الأوكراني حاليًا ما يقارب 70 شركة مملوكة للدولة، إلى جانب حوالي 400 شركة من القطاع الخاص، مما يعكس تنوعًا واتساعًا في القاعدة الصناعية الدفاعية. من بين هذه الشركات، تنخرط نحو 200 شركة في تطوير أنظمة غير مأهولة، تشمل البرية والجوية والبحرية، في حين تركز حوالي 50 شركة على تصميم وتطوير تقنيات الحرب الإلكترونية. بالإضافة إلى ذلك، تسهم ما يقرب من 150 شركة في إنتاج أنظمة تسليح متنوعة، مما يشير إلى نمو متكامل في مختلف مجالات الصناعات الدفاعية (Kuzio, 2024, p.1).

في عام 2023، أُطلقت مبادرة **BRAVE1** بقيادة وزارة التحول الرقمي الأوكرانية وبالتنسيق مع جهات عسكرية واستراتيجية، بهدف تسريع تطوير التقنيات العسكرية، خصوصًا الطائرات بدون طيار المزودة بالذكاء الاصطناعي. تُركّز المبادرة على تعزيز كفاءة القوات المسلحة من خلال دعم ابتكارات تشمل طائرات استطلاع وهجوم ونقل، إلى جانب طائرات إزالة الألغام. كما طوّرت برمجيات ذكية للرصد وتحديد الأهداف وتفادي التهديدات. ومن أبرز إنجازاتها الحديثة، اختبار تقنيات استراتيجية كأسراب المسيّرات، والذخائر الدقيقة، والروبوتات الشبيهة بالكلاب، ما يعكس تقدمًا نوعيًا في القدرات القتالية الأوكرانية (Samus & Artemenko, 2025, p.25).

شهدت صناعة الطائرات بدون طيار في أوكرانيا تطورًا نوعيًا خلال فترة الحرب، تجلّى في الارتفاع الكبير بمعدلات الإنتاج والابتكار. أذ ارتفع عدد الوحدات المُنتجة من نحو 3,000–5,000 في عام 2022 إلى ما يقارب 300,000 وحدة في عام 2023، في إطار استراتيجية موسّعة للحرب غير المأهولة. وتوظف أوكرانيا هذه الأنظمة بفعالية في ميادين برية وجوية وبحرية، حيث تُستخدم الروبوتات الأرضية للدعم اللوجستي والإجلاء الطبي،

فيما تسببت المركبات البحرية غير المأهولة بأضرار ملموسة لأسطول البحر الأسود (Mylovanov, 2024, p. 10-12) كما Bilousova, Omelchenko, Makarchuk &. طُوّرت نماذج متقدمة مثل "ماريتشكا" و"تولوكا"، بخصائص شبحية وقدرات اتصال فضائي مباشر (Kabanenko, 2024, p. 2) ، إلى جانب طائرة "فالكون-300" ذات المدى الطويل والحمولة الكبيرة. وقد مكّنت تلك القدرات أوكرانيا من تنفيذ هجمات دقيقة على أكثر من 200 هدف استراتيجي داخل الأراضي الروسية، مما يعكس التحول المتسارع في بنية الحرب المعاصرة نحو الأنظمة غير المأهولة (Rusya-Ukrayna, 2025,p 25).

بحلول عام 2024، أصبحت أوكرانيا من الدول الرائدة عالميًا في إنتاج الطائرات المسيّرة، بقدرة سنوية تقارب مليوني وحدة، متجاوزة العديد من دول الناتو. وقد مكّنها هذا التفوق من تنفيذ هجمات دقيقة على أهداف استراتيجية داخل روسيا، بدعم غربي تقني ومالي. وتعكس تلك العمليات، مثل استهداف مستودع نفط في بروليتارسك، فعالية المسيّرات منخفضة الكلفة في إحداث تأثيرات استراتيجية عميقة ضمن مشهد الحرب الحديثة (Kuzio, 2024, p. 1).

المبحث ألرابع: الأمن السيبراني والحرب الروسية الاوكرانية

توصف أوكرانيا كثيرًا بأنها منطقة نفوذ تاريخية لروسيا، كما تُعتبر ساحة اختبار رئيسية للهجمات السيبرانية الروسية وتجريب أدوات وتقنيات الاختراق. ففي عام 2015، تعرضت شبكة الكهرباء الأوكرانية لهجوم إلكتروني يُعرف باسم ""BlackEnergy، مما أدى إلى انقطاع التيار الكهربائي مؤقتًا عن نحو 80,000 من عملاء شركات الكهرباء في غرب البلاد. وبعد عام، وقع هجوم آخر يُدعى ""Industroyer، تسبب في انقطاع الكهرباء لمدة تقارب الساعة عن نحو خمس العاصمة كييف، تُعد تلك الهجمات جسا للنبض واستعراض للقدرات التي يبغي الروس ايصالها للجانب الأمريكي الغربي من حيث قوة الردع السيبراني التي يمتلكوها ، والتي اذا كان من الصعب للغاية تنفيذ هجمات إلكترونية على الأنظمة التقنية المعقدة بشكل موثوق اليوم لكن الغد بعد بتطور هائل للأسلحة السيبرانية داخل هذا الفضاء الجديد (فؤاد بنبوعزة ،٢٠٢٣، ص ٢٠٧).

يُعد هجوم " "NotPetya الإلكتروني من أكثر الهجمات تكلفة في التاريخ، وقد وُجّهت أصابع الاتهام فيه إلى مجموعة من القراصنة العسكريين الروس من قِبل الولايات المتحدة

والمملكة المتحدة وعدد من الدول الأوروبية. استُخدم في هذا الهجوم برنامج مدمر تم إخفاؤه داخل تحديث لبرنامج محاسبة واسع الاستخدام في أوكرانيا، لكنه سرعان ما خرج عن نطاقه المحلي وانتشر عالمياً، مُلحقاً أضراراً جسيمة بأنظمة الحواسيب لدى آلاف الشركات حول العالم، ومسبباً خسائر تُقدّر بنحو 10 مليارات دولار. ورغم أن أوكرانيا كانت الهدف الأساسي للهجوم بنسبة 80%، إلا أن تأثيراته امتدت لتشمل ألمانيا بنسبة تقارب 90%، إضافة إلى عدة دول غربية أخرى. وفي سياق الصراع القائم بين روسيا وأوكرانيا، رصد معهد السلام الإلكتروني 918 هجوماً إلكترونياً أو عملية سيبرانية مرتبطة بالحرب، وذلك حتى 13 كانون الأول 2023 (Bujon, 2022, p.36). إلا أن الهجمات السيبرانية الروسية ضد أوكرانيا لم تبدأ مع اندلاع الحرب الحالية، بل تعود إلى سنوات سابقة، حين تحوّلت أوكرانيا إلى ساحة لهجمات إعلامية وضربات إلكترونية استهدفت قطاعات حيوية، لاسيما قطاع الطاقة كما حدث بين عامي 2015 و2016، عندما أصيبت محطات الطاقة بالشلل لساعات. تلك الوقائع تبرهن على أن القدرات السيبرانية الروسية تمثل تهديداً فعلياً ومنظماً، وليست مجرد هجمات عشوائية أو مؤقتة. (de la guerre,2022, p.62-64).

يواصل الجانب الروسي تنفيذ استراتيجيته الردعية من خلال الاعتماد المكثف على ما يُعرف بـــ"هجمات رفض الخدمة" (DDoS) هي هجمات تقوم بإغراق الخوادم بطلبات وهمية لجعل المواقع غير متاحة، وقد استهدفت هذه الهجمات عدداً كبيراً من البنوك الأوكرانية والمؤسسات الحكومية. هذا النوع من الهجمات ليس بجديد، إذ سبق استخدامه في نزاعات سابقة مع دول مجاورة مثل جورجيا وإستونيا. إلى جانب ذلك، شنت روسيا هجمات سيبرانية أكثر تطوراً، من أبرزها استهداف نظام الأقمار الصناعية " "A-SATالمُستخدم من قبل الجيشين الأوكراني والألماني، وكذلك البنية التحتية لإدارة توربينات الرياح في أبريل الماضي (فؤاد بلبوعزة ،٢٠٢٣، ص ٢٠٨).

كما شهدت الساحة الإلكترونية تصعيداً من خلال استخدام برمجيات خبيثة من نوع "ممسحة" Wiper وهي فيروسات تُستخدم لمسح البيانات وتدميرها بشكل دائم. وتشير الباحثة كريستين دوغوين كليمان إلى أن هذا النوع من الهجمات بدأ منذ الأيام الأولى للحرب الروسية على أوكرانيا، ويُعد من أبرزها الهجوم المعروف باسم " "WhisperGate الذي استهدف مؤسسات أوكرانية رئيسية وأدى إلى شلّ نشاطها بشكل كبير (Bujon, 2022, p.37).

في ايار 2023، تصاعدت وتيرة الهجمات باستخدام البرمجيات الخبيثة من نوع "الممسحة" ((Wiper، وهي فيروسات تُستخدم لتدمير البيانات بالكامل، فإن روسيا بدأت هذا النوع من الهجمات منذ الأيام الأولى لحربها على أوكرانيا، ويُعد الهجوم المعروف بـــ" "WhisperGateمن أبرزها، إذ استهدف مؤسسات حكومية أوكرانية رئيسية وتسبب في شلل كبير لعملها. ولا تقتصر الحرب السيبرانية على الهجمات التقنية فحسب، بل تُستخدم أيضاً كأداة للحرب النفسية من خلال حملات التضليل الإعلامي التي تهدف إلى تشويه صورة الخصم، والتأثير في الرأي العام، إضافة إلى جمع المعلومات وتنفيذ ضربات استباقية لتهيئة بيئة الصراع لصالح الجهة المهاجمة (de la guerre,2022, p.65-67).

ويُعزى تقليل حجم القدرات السيبرانية الروسية إلى الدعم الكبير الذي تلقته أوكرانيا من الولايات المتحدة في السنوات الأخيرة، والذي بلغ ملايين الدولارات، وساهم في تعزيز قدراتها الدفاعية في الفضاء الإلكتروني. ومع ذلك، لا تزال الحرب الإلكترونية محاطة بالكثير من الغموض، نظراً لطبيعتها غير المرئية وصعوبة قياس تأثيرها بدقة (فؤاد بنبوعزة، ٢٠٢٣، ص٢٠٩).

اعتمدت روسيا على استراتيجية هجومية في المجال السيبراني كأداة فعالة لبسط سيطرتها على فضاءها المعلوماتي، ولإضعاف فضاءات المعلومات الخاصة بخصومها، وترتكز هذه الاستراتيجية على العقيدة العسكرية الروسية، التي تولي أهمية كبيرة للمرحلة التمهيدية التي تسبق العمليات العسكرية التقليدية، حيث يتم خلالها إنهاك العدو عبر استهداف بنيته المعلوماتية، وتعطيل قدرته على الوصول إلى البيانات، واختراق نظامه العام، بما يشمل البنية المالية، والمؤسسات الحكومية، وأنظمة الاتصالات، إلى جانب ذلك، تسعى روسيا إلى التأثير على الرأي العام للخصم من خلال نشر معلومات مضللة تُسهم في توجيه مسار الحرب والتأثير على دعم الجبهة الداخلية. وتعتمد هذه الاستراتيجية على محورين رئيسيين: الأول مادي يتصل بالجانب التقني مثل قرصنة الأجهزة والشبكات، والثاني معنوي يرتبط بالحرب النفسية وتوجيه الإدراك الجماعي (Willett, p.7).

اعتمدت روسيا على مجموعات قرصنة إلكترونية لتنفيذ هجماتها السيبرانية، مستهدفة الحسابات العسكرية والمدنية الأوكرانية بهدف اختراقها والحصول على معلومات حساسة، إضافة إلى الترويج لصورة إيجابية عن روسيا. ووفقًا لتقارير شركة "ميتا" التابعة لمارك

زوكربيرج، فإن إحدى هذه المجموعات، التي تُعرف باسم "كتاب الأشباح"، قامت بنشر مقاطع فيديو تحث الجنود الأوكرانيين على الاستسلام، كما عملت على بث أخبار كاذبة وتقارير مضللة، من بينها ادعاءات بانسحاب القوات الحكومية الأوكرانية وهروب قادتها خارج البلاد (Khoirunnisa، p142).

تلجأ روسيا إلى أجهزتها الاستخباراتية لتنفيذ بعض الهجمات السيبرانية، وقد رصدت شركة "مايكروسوفت" وتمكنت من التصدي لإحدى هذه الهجمات المعروفة باسم "سترونتيوم" ((Strontium، والتي تُنسب إلى وكالة الاستخبارات العسكرية التابعة لهيئة الأركان العامة الروسية. وتستهدف تلك الهجمات بشكل مباشر المؤسسات الأوكرانية، بالإضافة إلى مراكز الفكر في الولايات المتحدة والاتحاد الأوروبي، في إطار السعي لتحقيق أهداف تكتيكية تخدم المصالح الروسية (Willett, p.8).

اعتمدت روسيا على استخدام البرمجيات الخبيثة كوسيلة لاختراق الأنظمة المعلوماتية وتعطيل أجزاء حيوية من البنية التحتية الأوكرانية. ففي كانون الأول 2015، نفذت هجومًا باستخدام برامج خبيثة من نوع "ماسحة" استهدفت شركات توزيع الكهرباء، مما أدى إلى انقطاع التيار الكهربائي عن نحو 250 ألف مواطن أوكراني .ولم يقتصر تأثير هذا الهجوم على قطاع الطاقة، بل طال أيضًا مؤسسات أخرى مثل البنوك، والسكك الحديدية الوطنية، وخدمة البريد، ووزارة الصحة، وقدّر أحد المسؤولين الحكوميين الأوكرانيين أن نحو 10% من أجهزة الكمبيوتر في البلاد تأثرت بالهجوم، فيما أشارت شركة " Information Systems Security Partners"إلى أن 300 شركة أوكرانية تعرضت للاختراق نتيجة استخدام دودة إلكترونية ذاتية الانتشار وغير خاضعة للسيطرة. كما استُغلت ثغرة أمنية تعرف باسم "ثغرة تكنولوجيا المعلومات العالمية"، ما تسبب بأضرار جسيمة لأنظمة في 60 دولة أخرى، بما في ذلك الولايات المتحدة الأمريكية ودول أعضاء في حلف الناتو (Willett .p.9).

وتبرز من خلال هذا السياق أهمية حرب المعلومات والتضليل كجزء أساسي من الاستراتيجية الروسية في الهجوم على أوكرانيا. فبالرغم من استخدامها للوسائل العسكرية، اعتبرت موسكو أنها غير كافية لحسم الصراع وتحقيق أهدافها الجيوسياسية، التي لا تقتصر على أوكرانيا فقط، بل تشمل أيضًا محيطها الإقليمي وحلفاءها الدوليين ، وفي مواجهة الهجمات السيبرانية الروسية الممنهجة، تبنت أوكرانيا استراتيجية دفاعية محكمة تهدف إلى

التصدي لتلك التهديدات، وقد تجاوز تأثير هذه الاستراتيجية حدودها ليشمل دول حلف الناتو أيضًا. وقد استند هذا النهج الدفاعي إلى مجموعة من المحاور الأساسية التي شكلت أساسًا متينًا لتحصين الفضاء السيبراني الأوكراني وتعزيز قدرته على الصمود (Willett .p.9).

قامت أوكرانيا بالتعاون مع مجموعات قرصنة لتنفيذ هجمات سيبرانية هجومية استهدفت أنظمة الكمبيوتر الروسية، وذلك عبر تجنيد عدد من فرق القراصنة التي عملت على تعطيل مواقع تابعة لمؤسسات روسية، من بينها بنوك، مواقع إعلامية وحكومية، إضافة إلى شركات البث التلفزيوني والإذاعي المباشر ,وهدفت هذه العمليات إلى إزالة الحسابات والمحتويات الدعائية المؤيدة لروسيا من المواقع الإلكترونية الأوكرانية، إضافة إلى حماية البنية الرقمية الأوكرانية من هجمات القراصنة الروس، وذلك من خلال تعاون رسمي وشعبي، اعتُبر بمثابة خط دفاع أمامي في مواجهة حرب المعلومات التي تشنها روسيا ضد الرأي العام الأوكراني (Khoirunnisa, p .142).

أنشأت أوكرانيا أداة رقمية عسكرية تُعرف باسم "دلتا"، طوّرها فريق من المتطوعين المدنيين لتكون بمثابة نظام خدمات آمن مخصص لدعم الجيش الأوكراني. تهدف تلك الأداة إلى رقمنة العمليات العسكرية وتسهيل الإجراءات الداخلية، من خلال تقليص مستويات البيروقراطية التي تعيق سرعة التنفيذ. وقد تم دمجها مع تطبيق ""Diia، مما أتاح للمواطنين الأوكرانيين إمكانية الوصول إلى بعض خدماتها، تأخذ "دلتا" شكل خريطة جغرافية تفاعلية متعددة الطبقات، يمكن استخدامها عبر متصفح الإنترنت من خلال مختلف الأجهزة، سواء كانت هواتف ذكية، أجهزة لوحية، أو حواسيب شخصية (Kryvetska, 2025, p. 5).

لجأت أوكرانيا إلى التعاون مع أطراف دولية وإقليمية لمواجهة التهديدات السيبرانية الروسية، أذ استجابت عدة جهات غير حكومية تنشط في مجال الأمن السيبراني لدعوات الحكومة الأوكرانية، من بينها مجموعات من القراصنة المتطوعين الذين ساهموا في تنفيذ هجمات على البنية التحتية الرقمية الروسية. ومن أبرز هذه المجموعات، الفريق التابع لشبكة "Anonymousالذي أعلن مسؤوليته عن اختراق منصة الفيديو الروسية " "RuTube في أوائل مايو، مما أدى إلى تعطيلها لمدة يومين. كما قامت مجموعة " "NB65 باختراق وتعطيل خوادم عدد من شبكات التلفزيون الروسية، ضمن إطار الجهود الدولية لدعم أوكرانيا في التصدي للحرب السيبرانية الروسية (Government, 2022, p. 5).

النتائج

1. بدأ تطوير الذكاء الاصطناعي لأغراض الحرب قبل الصراع المسلح في أوكرانيا، في سياق التنافس الجيوستراتيجي بين الصين والولايات المتحدة، والذي ينطوي على إمكانية تغيير أسلوب خوض الحروب.
2. تُسرّع الحرب في أوكرانيا عملية تطوير الذكاء الاصطناعي لأغراض عسكرية، ورغم أن طبيعة الحرب لم تُحدد بعد من خلال الذكاء الاصطناعي، إلا أن الحرب بين روسيا وأوكرانيا تُشبه مختبرًا تُمكّن العديد من الشركات والحكومات من تدريب واختبار أنظمة الذكاء الاصطناعي باستمرار لمجموعة واسعة من القدرات والوظائف والتطبيقات.
3. دمج كلا الجانبين الذكاء الاصطناعي لتعزيز فعالية الطائرات بدون طيار وغيرها من التقنيات، سعياً لتحقيق تفوق تكتيكي وعملياتي في ساحة معركة ديناميكية تعتمد بشكل متزايد على التكنولوجيا.
4. يمثل تطور الذكاء الاصطناعي في المجال العسكري الروسي استراتيجية مدروسة وطويلة الأمد لتعزيز القدرات العملياتية والحفاظ على التكافؤ الاستراتيجي في الحروب الحديثة. تقدمت أبحاث الذكاء الاصطناعي الروسية لتشمل أحدث التقنيات في تطبيقات متنوعة، من الطائرات بدون طيار إلى المنصات الأرضية الروبوتية.
5. تُبرز الادعاءات الموجهة ضد روسيا بشأن نشر أنظمة مدعومة بالذكاء الاصطناعي لأغراض عسكرية، بما في ذلك الطائرات بدون طيار والهجمات الإلكترونية، الطبيعة المتطورة للحرب الحديثة ودمج التقنيات المتقدمة في الاستراتيجيات العسكرية. وبينما وفرت هذه التكتيكات المدعومة بالذكاء الاصطناعي بلا شك مزايا تكتيكية من حيث السرعة والدقة، فإنها تُثير أيضًا مخاوف أخلاقية كبيرة وتُؤكد على الحاجة المُلحة إلى لوائح وإرشادات دولية تُنظّم تطوير الذكاء الاصطناعي واستخدامه في التطبيقات العسكرية.
6. يُمثّل الصراع الروسي الأوكراني دراسة حالة وجيهة لتقييم المخاطر والفوائد المرتبطة بالذكاء الاصطناعي في الحروب. فمن ناحية، أتاح استخدام الأنظمة المدعومة بالذكاء الاصطناعي شنّ هجمات أكثر كفاءة وتنسيقًا، مما قد يُغيّر

ديناميكيات الحرب. ومن ناحية أخرى، أثار مخاوف بشأن المساءلة، وسقوط ضحايا مدنيين، واحتمالية حدوث عواقب غير مقصودة.

7. ومن خلال إعطاء الأولوية لتطوير الذكاء الاصطناعي المسؤول والالتزام بالمعايير الدولية، يمكن للمجتمع الدولي أن يعمل على ضمان مساهمة تقنيات الذكاء الاصطناعي في الأمن والاستقرار العالمي مع الحفاظ على المبادئ الأساسية للأخلاق وحقوق الإنسان.

المصادر

اولاً: المصادر العربية

1. أسامة ابو رشيد، الأزمة الأوكرانية، إعادة بعث الحرب الباردة، قطر، المركز العربي للأبحاث والدراسات السياسية، ٢٠١٤.
2. باسم راشد، تهديد جيواستراتيجي حسابات القطب الروسي بالأزمة الأوكرانية، القاهرة، مجلة السياسة الدولية، مركز الأهرام للدراسات السياسية والإستراتيجية، القاهرة، العدد 169، ٢٠١٤.
3. عبد الغني أماني غالب، نضال الشعوب الثائرة، نماذج حول العالم ، مركز المصري للدراسات والمعلومات، القاهرة، ٢٠١٣.
4. فؤاد بنبوعزة ، الحرب السيبرانية الروسية الأوكرانية بين التنظير والواقع الميداني ، المجلة العسكرية الاستراتيجية ، العدد ٢٠، إصدارات المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين ، ٢٠٢٣.
5. محمود عبد العاطي، عودة النفوذ الروسي في أوروبا الشرقية ، مجلة السياسة الدولية، العدد 1، مركز الأهرام، القاهرة، ٢٠١٠.
6. نافع بشير، الأزمة الأوكرانية تفجر الصراع على أوروبا من جديد، قطر، مركز الجزيرة للدراسات، ٢٠١٤.
7. ياسين أشرف محمد عبد الله ، الثورة والتحول الديمقراطي في دول الموجة الرابعة للديمقراطية (دراسة للثورات الانتخابية ، مجلة بحوث الشرق الأوسط، العدد 38، ج1، د. ت.

8. يسرى الشرقاوي، الشراكة الشرقية تكفير الاتحاد الأوروبي عن أخطائه، مجلة السياسة الدولية، مركز الأهرام، القاهرة، العدد ٢٠٠٩،.

ثانياً: المصادر الأجنبية

أ- المصادر الانكليزية

1. Anu Sharma, Drone Warfare in the Russia-Ukraine War, International Journal of Humanities Social Science and Management (IJHSSM), Volume 5, Issue 2, Mar.-Apr., 2025.
2. Bilousova, O., Omelchenko, E., Makarchuk, M. & Mylovanov, T. Ukraine's Drones Industry: Investments and Product Innovations. 2024.
3. Bilousova, O., Zagrebelska, A., Vlasiuk, V. & Shapoval, N. Foreign Components in Russian Military Drones, Yermak-McFaul International Working Group on Russian Sanctions, 23 August 2023.
4. Bujon, Anne-Lorraine, et Marie Mendras. En Ukraine et en Russie, le temps de la guerre. Introduction, Esprit، no. 4, 2022.
5. de la guerre en Ukraine sur le secteur russe du numérique, Revue d'économie financière, vol. 147, no. 3, 2022.
6. Eslami, M. Iran's Drone Supply to Russia and Changing Dynamics of the Ukraine War. Journal for Peace and Nuclear Disarmament 5, 2022.
7. Favaro, M., & Williams, H. False sense of supremacy: emerging technologies, the war in Ukraine, and the risk of nuclear escalation. Journal for Peace and Nuclear Disarmament, 6(1)، 2023.
8. Government of, c. Cyber threatbulleitn: Cyber threat Activity Related to the Russian of Ukraine. Canadian Centre for Cyber Security, 2022.
9. Hall, R. C. Reconnaissance drones: their first use in the cold war. Air power history Vol. 61, No. 3، 2014.
10. Hamad, A. M. & Alaiwi, Y. Localization and identification of UAVs system using image processing. 27 June 2022, Turkey.
11. Iranian UAVs in Ukraine: A Visual Comparison, DEFENSE INTELLIGENCE AGENCY, August 2023.
12. Kabanenko, I. Ukraine Restoring Security to the Black Sea. Eurasia Daily Monitor Volume: 21 Issue: 37, 2024.

13. Khoirunnisa, C. S. Cyber Warfare Strategies in the Russia-Ukraine Conflict(2021-2022): Implications for National Security and Modern Warfare , Jurnal Public Policy,vol 10, no (2).
14. Kinik, H. & Çelik, S. The Role of Turkish Drones in Azerbaijan's Increasing Military Effectiveness. Insight Turkey 23، 2021.
15. Kryvetska, A. cyberguerre et nouvelles technologies: les civils sont-ils un moyen asymétrique redoutable dans la guerre en Ukraine ?,. la revue géopolitique, 2025.
16. Kuzio, T. Ukraine Leads World in Drone Innovation and Production. urasia Daily Monitor Volume: 21 Issue: 145, 2024.
17. Kuzio, T. Ukraine Leads World in Drone Innovation and Production. urasia Daily Monitor Volume: 21 Issue: 145, (2024).
18. Mykhailo Samus, Oleksandra Artemenko, The Impact of Artificial Intelligence in the Drones' War in Ukraine, New Strategy Center, 2025 .
19. Nafuye Ivan, Weaponizing Artificial Intelligence in the Russia-Ukraine war, Department of Information technology, Uganda Christian University, 2024.
20. Paul Scharre, Army of None: Autonomous Weapons and the Future of War, W. W. NORTON & COMPANY, New York, London, 2018.
21. Pavel Luzin, RUSSIA'S SPACE PROGRAM AFTER 2024, the Foreign Policy Research Institute, July 2024.
22. Pettyjohn, S., Dennis, H. & Campbell, M. Swarms over the Strait Drone Warfare in a Future Fight to Defend Taiwan, JUNE 2024.
23. Richter, W , NATO-Russia Tensions: Putin Orders Invasion of Ukraine: With the European Security Order in Shambles.SWP Comment, No.(16), March,2022.
24. Stracker, Matthew. An Operational Manpower Analysis of the RQ-8 Fire Scout Vertical Take-Off Unmanned Aerial Vehicle (VTUAV). Thesis, Monterey: Naval Postgraduate School, 2007.
25. Willett, M. The Cyber Dimension of the Russia-Ukraine War. Survival Global Politics and Strategy,vol 64 , no(5).
26. William M. Arkin, Unmanned: Drones, Data, and the Illusion of Perfect Warfare, New York : Little, Brown and Company, 2015.

27. Youvan, D. C. Downing the MQ-9 Reaper: Analyzing Yemen's Air Defense Tactics and Capabilities in Modern Warfare, 10 September 2024.

ب- التركية

1. Ateş, E. Türkiye'nin İnsansız Hava Aracı (İHA) ihracat rekabet gücünün analizi. Türkiye İnsansız Hava Araçları Dergisi 3, 7–16 (2021).
2. Göktürk Çetinkaya, S., & Koç, M. Türkiye'nin İnsansız Hava Araçları Serüveni. Anadolu Strateji Dergisi, 5(1)،2023.
3. RUSYA-UKRAYNA SAVAŞI'NDA İHA KULLANIMI:MODERN SAVAŞIN YENİ OYUNCULARI VE GELECEĞİN TEKNOLOJİK DÖNÜŞÜMÜ, Millî İstihbarat Akademisi، TÜRKİYE،2025.

ج- الروابط الالكترونية

1. Russia Was Lagging Behind in Drone Capabilities but Is Now Catching Up: Comment (2023). https://www.lrt.lt/en/news-in-english.