الحرب الالكترونية والذكاء الاصطناعي : دراسة في الاستراتيجيات المعاصرة للأمن القومي

ا.م.د. ظفر عبد مطر التميمي

الجامعة المستنصرية / كلية العلوم السياسية

thafarmatar@gmail.com

https://orcid .org/
0000-0003-2404-027X

الملخص :

شهد النصف الثاني من القرن العشرين، خصوصا في عقوده الثلاثة الأخيرة ثورة علمية في الاختراعات والمكتشفات الحديثة في كافة المجالات، وقد حظي المجال العسكري منها بالنصيب الأكبر لهذه الاختراعات والمكتشفات، مثل:الأسلحة، والمعدات الحربية، وأدوات الصراع المسلح ، والتي تعمل لصالح جميع أنواع القوات المسلحة البرية، والبحرية، والجوية، والدفاع الجوي ، ووسائط الحرب الالكترونية، فضلا عن التطور الهائل الذي لحق بوسائط الحرب النووية ، وأسلحة التدمير الشامل وغيرها. ويواجه الأمن القومي كنتيجة لذلك التطور الهائل المزيد من التهديدات والمخاطر المرتبطة بتطوير تقنيات وأدوات الذكاء الاصطناعي في الحروب الالكترونية، والتي قد تؤثر على الاستقرار العالمي، رغم الفوائد الكثيرة المصاحبة لاستخدامها، إذ تتنافس الدول على تطوير أنظمة الذكاء الاصطناعي وسن التشريعات والقوانين لتنظيم استخدامه. أن الحروب الالكترونية ستتطور بالتأكيد لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل، فلقد أعاد الذكاء الاصطناعي صياغة أساليب خوض الحروب، والحفاظ على الأمن ليشكل قوة حاسمة في ساحة المعركة ، وأصبح محوريا في الاستراتيجيات العسكرية الحديثة، بدءا من الطائرات المسيرة ذاتية التشغيل، وأنظمة المراقبة المتطورة، إلى

الـدفاع السـيبراني، ومـن هنـا تنبـع رغبتنـا فـي كتابـة هـذه الدراسـة والبحـث فـي الاستراتيجيات المعاصرة للأمن القومي، بعد اعتماد الذكاء الاصطناعي كقوة رئيسة في تحديد المنتصر في الحرب الالكترونية .

الكلمات المفتاحية :- الحرب الالكترونية – الذكاء الاصطناعي – الأمن القومي – الإستراتيجية – القوة العسكرية

Cyber Warfare and Artificial Intelligence: A study in Contemporary National Security Strategies

Assistant prof. dr. Dhufr Abed Mutar Al Tamimi
At the College of Political Science / Mustansiriyah University

E-mail :- thafarmatar@gmail.com
https://orcid .org/
0000-0003-2404-027X

Abstract :-

The second half of the twentieth century, especially in its last three decades, witnessed a scientific revolution in modern inventions and discoveries in all fields, the military field received the largest share of these inventions and discoveries, such as: weapons, military equipment, and tools of armed conflict, which work for the benefit of all types of land, sea, air, and air defense armed forces, and electronic warfare equipment.

In addition to the tremendous advancements in nuclear warfare, weapons of mass destruction, and other related technologies, national security faces increasing threats and risks associated with the development of artificial intelligence technologies and tools in cyber warfare. These advancements, despite its numerous benefits, could impact global stability ,as

countries compete to develop artificial intelligence systems and enact legislation to regulate their use . Cyber warfare will undoubtedly evolve into a decisive weapon in future conflicts between nations, artificial intelligence has reshaped the methods of waging war and maintaining security, becoming a crucial force on the battlefield . It has become central to modern military strategies , from autonomous drones and advanced surveillance systems to cyber defense . Hence our desire to write this study and research contemporary national security strategies, after the adoption of artificial intelligence as a major force in determining the victor in electronic warfare.

Keywords:- Cyber warfare , Artificial intelligence , National security , Strategy , Military power .

المقدمة :-

يشهد المجال العسكري تطورات مهمة بشكل متسارع ، وهو ما يتطلب من الدول كافة الاستفادة من التطوير الحاصل في الميدان العسكري، وخاصة الذكاء الاصطناعي الذي يعد القمة فيما وصل إليه العلم التطبيقي، والذي بدأ يأخذ طريقه ليس فقط في المجال العسكري والأمني، بل توسع إلى مجالات الحياة الأخرى ، بكل ما يحمله ذلك من فرص وتحديات وعلى أكثر من مستوى ، وقد جاء استخدام الانترنت كوسيلة في الحرب الالكترونية (المعلوماتية)، والتي تشمل استخدام سلاح المعلوماتية سواء كانت من خلال الانترنيت أو القنوات الفضائية أو وسائل الإعلام الأخرى المسموعة والمرئية وغيرها ، او استخدامه لتوجيه أسلحة او لتعطيل دفاعات الطرف المعادي ، او للتحكم في التوجيهات او المعلومات التي يجب أن يتم انتقالها عبر الشبكات ، وغير ذلك من الوسائل المؤثرة على الصراع .

ولم تعد القوة تقاس فقط بالعوامل المادية، بل أصبحت القدرات السيبرانية عنصرا حاسما ، ويثير استخدام كل هذه التقنيات، وخاصة تقنيات الذكاء

الاصطناعي في عدد من ساحات الصراع المسلح مثل: الحرب الروسية الأوكرانية، والحرب الإسرائيلية في غزة، والعدوان الأمريكي الإسرائيلي على الجمهورية الإسلامية الإيرانية حاليا ، العديد من النقاشات المتتالية في الاستراتيجيات المعاصرة للأمن القومي ، وذلك حول ماهية تلك الاستخدامات ، ومخاطرها على الأمن الإقليمي والعالمي ، واستدامة الصراع ، إذ أظهرت تلك التجارب ، أن الأسلحة المدعومة بالذكاء الاصطناعي يمكن أن تكون أكثر دقة من الأسلحة الموجهة باليد البشرية ، مما قد يقلل من الأضرار الجانبية ، كالضحايا المدنيين ، والأضرار بالنية التحتية ، وأعداد الجنود المستهدفون ، بينما تساعد الدول والمجموعات الضعيفة على الدفاع عن نفسها، في حين قد تؤدي في ذات السياق إلى ارتكاب العديد من الأخطاء الكارثية التي لا يمكن إصلاحها أو تعويضها .

الأهمية :-

ترتكز أهمية البحث ، في كونه يلقي بالضوء على الاستراتيجيات المعاصرة للأمن القومي ، التي انشر مفهومها بشكل أوسع بعد استخدام ودمج الذكاء الاصطناعي بالحروب الالكترونية ، وذلك اثر المنافسة على النفوذ، التي اخترقت وحدات النظام العالمي ، فظهرت لتلك الحروب تطبيقات واسعة في عدة مناوشات وحروب حديثة ، مما أدى إلى تغير مفاهيم مثل : الإستراتيجية ، والأمن القومي ، والصراع ، والمواجهة العسكرية المباشرة .

الهدف :- يهدف البحث إلى بيان أهمية الذكاء الاصطناعي والمعلوماتية في صياغة الاستراتيجيات الخاصة بالأمن القومي ، وانعكاسها على ارض الواقع بشكل يختلف عن الاستراتيجيات التقليدية ، مع بيان الأضرار التي تخلفها النزاعات والحروب الالكترونية ، ومدى انسجامها مع العقيدة العسكرية التقليدية في ضوء تطورها وانتشارها ، نتيجة تزايد ارتباط العالم بالذكاء الاصطناعي .

الإشكالية :-

ينطلق البحث من إشكالية تتعلق بقدرة الذكاء الاصطناعي والحروب الالكترونية على التأثير على الاستراتيجيات المعاصرة للأمن القومي ، ونقل علاقات القوى بين الوحدات الدولية إلى مستوى جديد ومختلف ، فضلا عن استخدامها في الحروب كعامل حاسم ، ومن ذلك يمكننا طرح عدة تساؤلات ، لعل من أهمها :-

١. ماهية الذكاء الاصطناعي والحروب الالكترونية ، وأسباب نشأتها ؟
٢. انعكاس استخدام الذكاء الاصطناعي والحروب الالكترونية على النظام العالمي الجديد ؟
٣. كيف أثرت الحروب الالكترونية على الاستراتيجيات المعاصرة للأمن القومي ؟

الفرضية :-

لقد بني البحث على افتراض ينص على:- (انه إذا تم اعتماد الذكاء الاصطناعي في الحروب المستقبلية ذات الصفة الالكترونية ، فان ذلك سينتج لنا استراتيجيات أمن قومي جديدة ، ستغير في توزيع ادوار القوى ، ونظام القطبية ، والمواجهة العسكرية ، وستكون سببا في إعادة رسم خرائط القوة للنظام العالمي الجديد) .

المنهجية :-

تم الاعتماد على منهجية التحليل الوصفي لمفهومي الذكاء الاصطناعي والحروب الالكترونية ، للوصول للنتائج المتوخاة من البحث .

الهيكلية :-

لأجل توضيح مفردات ومفاهيم البحث للقارئ والباحث ، فقد تم تقسيم البحث إلى ثلاثة محاور رئيسة ، هي :-

المحور الأول :- الإطار النظري وتطور مفهوم الحروب الالكترونية .

المحور الثاني :- الذكاء الاصطناعي .. المرونة في التوظيف العسكري .

المحور الثالث :- الاستراتيجيات المعاصرة للأمن القومي وأدوات المواجهة المستقبلية .

الخاتمة .

المحور الأول :- الإطار النظري وتطور مفهوم الحروب الالكترونية .

عرفت الحرب على أنها: عمل سياسي تقوم به دولة ما للدفاع عن المصالح أو الحقوق ، عند استنفاد بقية الوسائل الأخرى، إذ تلجأ إلى القوة المسلحة لتبرهن على قوتها، وقدرتها على فرض إرادتها ، كما تم تعريف الحرب، بأنها: أية معركة تم الاستعداد لها مسبقا، والقيام بالإعلان عنها من قبل حكومة شرعية، أو كيان يشابه الحكومة ، ويترتب عليها مقتل ما لا يقل عن ألف شخص، وذلك دون احتساب الضحايا غير المباشرين للحرب ، والذين قد يكونوا ضحايا محتملين، نتيجة للمجاعة أو الأمراض . [١]

أما الحرب الالكترونية، فيختلف المختصون بالشأن السياسي حول وضع تعريف محدد ودقيق لها، إذ عرفها **ريتشارد كلارك***بأنها: أعمال تقوم بها دولة ، لتحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها، فيما هناك تعريف آخر وهو أنها: مجموعة الإجراءات التي تقوم بها القيادة العامة والأفرع الرئيسة للقوات المسلحة، والأسلحة

*ريتشارد كلارك :- المستشار السابق لشؤون مكافحة الإرهاب في مجلس الأمن الأمريكي ومن أبرز الخبراء **الدوليين في مجال الأمن، بما في ذلك الأمن الداخلي، الأمن القومي، الأمن الإلكتروني ومكافحة الإرهاب، ويعمل كلارك حاليا كمستشار التغطية المباشرة لشبكة أي بي سي للأخبار، ومحاضر في كلية كنيدي للدراسات الحكومية في جامعة هارفرد، فضلا عن كونه عضو مجلس أمناء جامعة خليفة في الإمارات العربية المتحدة .**

[1] **. Johan M.G. van der Dennen, On War: Concepts, Definitions, Research Data - A Short Literature Review and Bibliography, University of Groningen, 2005, https://bit.ly/2VvgDWl .**

والتشكيلات ضمن النظم الالكترونية التي يستخدمها العدو في القيادة والسيطرة على قواته وأسلحته ومعداته، ومقاومة استطلاع العدو اللاسلكي والراداري وتحقيق استقرار في عمل النظم الالكترونية التي تستخدمها القوات المسلحة في القيادة والسيطرة ، وذلك تحت ظروف استخدام العدو لأعمال الإعاقة الالكترونية، وهو ما يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع عالمي . [٢] وتعني عبارة الحرب الالكترونية أيضا ، استخدام التقنيات الالكترونية المعروفة على اختلاف أنماطها في مواجهة أنظمة السلاح التي يملكها الخصم أو العدو .[٣]

كما تعرف بأنها : حرب تخيلية او افتراضية ذات طبيعة غير ملموسة تحاكي الواقع بشكل شبه تام ، وتكون بلا دماء ، إذ تتلخص أدوات الصراع فيها بالمواجهات الالكترونية والبرمجيات التقنية وجنود من برامج التخريب المحوسب وطلقاتها هي لوحات المفاتيح ونقرات المبرمجين في بيئة اصطناعية تحاول ما أمكن الوصول إلى صورة حقيقية لملامح الحياة المادية والملموسة . [٤] وكذلك تعرف الحروب الالكترونية: بكونها المشهد الصراعي المستقبلي والقادم للبشرية ولكن بصورة رقمية وتكنولوجية ، فهي صراعات قديمة جديدة بدأت منذ الوقت الذي ابتكر فيه الإنسان أدوات تواصله الأولى ، كالأصوات والتلغراف والهواتف اللاسلكية وأنظمة البرق الصوتي وأنظمة الترميز وآلات الطباعة وغيرها ، والتي تم

---

٢. إبراهيم إسماعيل كاخيا : الحرب الالكترونية ، مجلة الدفاع العربي ، المكتبة الالكترونية :- http://www.arabdefencejournal.com
وللمزيد ينظر في :- أشرف صلاح الدين: الانترنت.. عالم متغير ، ط١، مركز الحضارة العربية ، القاهرة ، مصر ، ٢٠٠٣.

٣. كمال السعدي : الحرب الالكترونية ، ط١ ، المركز العربي للدراسات الإستراتيجية ، المؤسسة العربية للدراسات والنشر ، بيروت ، لبنان ، ١٩٧٧ ، ص٩ .

٤ . كمال مساعد : الحرب الافتراضية وسيناريوهات محاكاة الواقع ، مجلة الجيش اللبناني ، ع ٢٥٣ ،٢٠٠٦ ، المكتبة الالكترونية :- https://www.leparmy.gov.Ib/artical.asp

استخدامها في الحربين العالميتين الأولى والثانية وما سبقهما من حروب وثورات وقعت في عقدي الثورة الفكرية والصناعية . [٥]

وتقوم الحروب الالكترونية بالدرجة الأولى على عنصرين مهمين ، هما :- [٦]

أولا :- توفر المعلومات التي ترتكز عليها الحروب التكنولوجية بشكل كبير ، إذ إن توفر عنصر المعلومات هو أول آليات عمل الحروب الالكترونية .

ثانيا:- القدرات العقلية والذهنية والتي تكون مسؤولة عن تخطيط وتوجيه الضربات الالكترونية والإجراءات الفنية والتقنية في عالم رقمي شديد التعقيد .

إن المجالات العسكرية هي واحدة من أكثر البيئات تجانسا والتصاقا بالحروب الالكترونية ، وهنا تعرف الحروب الالكترونية تبعا لترابطها بالقوة العسكرية بأنها: الحروب التي تتسم بالتعاون مع المؤسسة العسكرية ، إذ أنها تصوب نيرانها باتجاه الأهداف الالكترونية والرقمية والمعلوماتية ، كالتجسس على المعلومات والإشارات الصادرة من الأجهزة الالكترونية التابعة لأهداف العدو ، وتتبع الموجات القادمة من الاتصالات اللاسلكية وغيرها ، كما تستهدف المصالح القومية والسياسية والعسكرية والأمنية للدول المعادية ، متخذة شكل هجمات واختراقات الكترونية لتعطيل البنية المعلوماتية . [٧]

بدأت مظاهر الحرب الإلكترونية تاريخيا قبل اندلاع الحرب العالمية الأولى، إذ تتم الاتصالات باستخدام المواصلات السلكية من طريق المورس (جهاز البرق الصوتي) عام ١٨٣٧ ، ثم تبادل المراسلات باستخدام السفن في نقل الرسائل بين

---

٥. عبد الكريم صالح المحسن : ساحة المعارك العظمى التالية : الفضاء الالكترونية ، الحوار المتمدن ، محور الأبحاث السياسية ، ع ٣٦٠٤ ، ٢٠١٢ ، المكتبة الالكترونية :- https://www.ahewar.org/debat/shoe.art.asp

٦. صفات سلامة : أسلحة حروب المستقبل بين الخيال والواقع ، مركز الإمارات للدراسات والبحوث الإستراتيجية ، ط١، أبو ظبي ، الإمارات العربية المتحدة ، ٢٠٠٥، ص ٣٨.

٧. عباس بدران : الحرب الالكترونية .. الاشتباك في عالم المعلومات ، مركز دراسات الحكومة الالكترونية للنشر والتوزيع ، بيروت ، ٢٠١٠، ص٣٠.

الموانئ البحرية ، ومنذ اندلاع الحرب الأهلية في الولايات المتحدة الأمريكية في عام ١٨٦١، إذ كانت خطوط التلغراف هدفا مهما للقوات المتحاربة ، وكان عمال الإشارة يتداخلون على خطوط المواصلات السلكية، من طريق توصيل هاتف على التوازي مع كل خط من هذه الخطوط للتنصت على المحادثات ، ولهذا السبب، كان كل جانب يقطع المواصلات الخطية عند عدم الحاجة إليها، حتى لا يتداخل عليها الطرف الآخر . [٨]

وارى كباحثة ، بأن الحروب الالكترونية هي نتاج طبيعي للتقدم التقني الحاصل، ومع ذلك، فان الصناعات العسكرية المتقدمة لن تستطيع حسم المعارك لطرف واحد، بسبب الانتشار والتقليد الواسع لتلك الصناعات وتعرضها للسرقة من دول وأطراف أخرى ، وهنا سنصل إلى حالة صفرية من المواجهة العسكرية ، وقد نصل يوما ما إلى ردع الكتروني قائم على توازن الأطراف المتصارعة في امتلاكها لنفس المستوى من القوة الالكترونية .

وهناك من يربط مفهوم الحرب الالكترونية ببيئة الانترنت فقط ، كونها ساعدت على انتشار المعلومات في مختلف أرجاء العالم بشكل كبير وسهلت الوصول إليها بشكل سريع بحيث يمكن تعريف الحروب الالكترونية بناء على ذلك بأنها الحرب التي تستهدف المعلومات ، بين أطراف متناقضة الأهداف ومتعارضة المصالح ومختلفة المواقف . [٩] وقد شكل التطور الالكتروني الذي شهده عالم التكنولوجيات الرقمية والالكترونية الكونية تنافسات شديدة ، إذ تتسم هذه الحروب بالسرية نوعا ما، وقلة التكاليف، ومرونة الوقت ، وسرعة الأداء ، وقوة

[٨] . موسوعة مقاتل من الصحراء ، المكتبة الالكترونية :- http://www.moqatel.com
[٩] . جعفر جاسم :حرب المعلومات بين أرث الماضي وديناميكية المستقبل ، ط١ ، دار البداية للنشر والتوزيع ، عمان ، الأردن ، ٢٠١٠، ص ٤٤-٦٥ .

التأثير ، وشبه انعدام معرفة هوية المهاجم والخلفيات الإيديولوجية ، وغيرها مما يجعلها شديدة الخطورة . [١٠]

وتتنوع مجالات وأشكال النزاع التي تحصل في الفضاء الإلكتروني، ومنها:- [١١]

١. **التخريب الإلكتروني** :- أو القرصنة الإلكترونية ، ويوجد في المستوى الأول من النزاع في الفضاء الإلكتروني، ويشمل القيام بتعديل أو تخريب أو إلغاء المحتوى أو تغيير طبيعته ، مثل القيام بعمليات قرصنة المواقع الإلكترونية أو بتعطيل الحواسيب الخادمة أو ما يعرف باسم الملقمات (Servers) من خلال إغراقها بالبيانات المزيفة .

٢. **الجريمة والتجسس الإلكتروني** :- وهما في المستوى الثاني والثالث وغالبا ما يستهدفان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات الحكومية .

٣. **الإرهاب الإلكتروني:**- وهو في المستوى الرابع من النزاع في الفضاء الإلكتروني ، ويستخدم لوصف الهجمات غير الشرعية التي تنفذها مجموعات أو فاعلون من خارج الحكومة (Non-State Actors) ، بالضد من أجهزة الكمبيوتر والشبكات والمعلومات المخزنة ، ولا يمكن تعريف أي هجوم إلكتروني بأنه إرهاب إلكتروني إلا إذا انطوى على نتائج تؤدي إلى أذى مادي للأفراد أو الممتلكات والى دمار يترك قدرا كبيرا من الخوف والشعور بالهزيمة .

٤. **الحرب الإلكترونية** :- وهي المستوى الأخطر للنزاع في الفضاء الإلكتروني، وتعد جزءا من الحرب المعلوماتية بمعناها الأوسع، وتهدف إلى التأثير على الإرادة السياسية للطرف الآخر، وعلى قدرته في عملية صنع القرار، وكذلك

[١٠] . وليد غسان سعيد جلعوط : دور الحروب الالكترونية في الصراع العربي الإسرائيلي ، رسالة ماجستير غير منشورة ، جامعة النجاح الوطنية ، فلسطين ، ٢٠١٣، ص٧٥.
[١١] . إبراهيم إسماعيل كاخيا: مصدر سبق ذكره .

التأثير فيما يتعلق بالقيادة العسكرية و/أو توجهات المدنيين في مسرح العمليات الإلكتروني .

٥. **الدعاية السلبية:**- رسائل سياسية يمكن نشرها لأي شخص يستخدم الإنترنت .

٦. **جمع البيانات** :- أي أن المعلومات السرية غير المحفوظة بأمان يمكن اعتراضها والتقاطها بل وتعديلها، مما يجعل التآمر في هذه الحالة ممكنا حتى من الجانب الآخر من العالم .

٧. **تعطيل المعدات العسكرية** :- الأنشطة العسكرية التي تستعمل الحواسب والأقمار الصناعية للتنسيق هي في خطر من هذا النوع من الهجمات، إذ يمكن اعتراض الأوامر والاتصالات أو استبدالها مما يعرض حياة الجنود للخطر .

٨. **مهاجمة البنى التحتية الحساسة** :- أي شبكات الكهرباء والماء والوقود والاتصالات والمواصلات ، ويمثل هذا التدمير الاقتصادي الأشد وطأة في حالاته القصوى .

خصائص الحروب الالكترونية ، ومنها:- [١٢]

١. **لا تناظرية** :- فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب يعني عدم الحاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة جدا كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا على دولة قوية .

٢- **أفضلية المهاجم** :- يتمتع المهاجم بأفضلية واضحة وكبيرة على المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة .

٣- **فشل أنموذج الردع** :- يعد مفهوم الردع الذي تم تطبيقه بشكل أساس في الحرب الباردة غير ذي جدوى في حروب الإنترنت ، فالردع بالانتقام أو العقاب لا ينطبق على هذه الحروب ، فعلى عكس الحروب التقليدية ، إذ ينطلق الصاروخ

[١٢] . إبراهيم إسماعيل كاخيا: المصدر السابق .

من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد الهجمات الإلكترونية ذات الزخم العالي ، وبعض الحالات قد تتطلب أشهرا لرصدها وهو ما يلغي مفعول الردع بالانتقام وكثير من الحالات لا يمكن تتبع مصدرها في المقابل، وحتى إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير حكوميين، فانه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها .

٤- **المخاطر تتجاوز المواقع العسكرية:-** هناك جهود متزايدة لاستهداف البنى التحتية المدنية والحساسة ، وهو أمر أصبح واقعيا في ظل القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادية حقيقية تؤدي إلى انفجارات أو دمار هائل .

ويلاحظ انه ، في مجال أعمال الحرب الإلكترونية الدفاعية (Defensive Measures) يوفر الاستطلاع الإلكتروني رصيدا من المعلومات عن الأوضاع والتحركات في مسرح العمليات ، وكذلك خصائص معدات العدو الإلكترونية، لاتخاذ الإجراءات الإلكترونية المضادة لمواجهتها ، كما يتيح التعرف على نظم المواصلات، وشبكات المعلومات التي تربط مراكز قيادة العدو بتشكيلاته ووحداته، وفي ذات الوقت ، يتم اتخاذ الإجراءات الكفيلة بتحقيق أمن السيطرة على المواصلات الصديقة، وعدم تمكين العدو من التداخل عليها ، أما في مجال أعمال الحرب الإلكترونية الهجومية (Offensive Measures) يركز في بداية العمليات على تدمير مراكز الحرب الإلكترونية المعادية بما يتيح حرية عمل الأسلحة الصديقة الموجهة، وتحقيق الدقة في إصابتها لأهدافها ، ويعد إبطال فاعلية مواصلات مراكز القيادة والسيطرة الآلية المعادية عن طريق الإجراءات الإلكترونية المضادة الصديقة، في مقدمة أولويات الحرب الإلكترونية ، لذلك يجري

التخطيط لذلك مسبقا قبل بدء العمليات، فإخماد أو إبطال عمل مراكز القيادة والسيطرة المعادية مبكرا يعني النهاية للحرب، وهو ما أثبتته عمليات الحرب الإلكترونية التمهيدية الناجحة للطائرات الحليفة في عملية (عاصفة الصحراء) في حرب الخليج الثانية . [١٣]

واجد كباحثة في هذا المجال، بان العدوان الأميركي – الإسرائيلي الأخير على الجمهورية الإسلامية الإيرانية قد امتلك معظم الخصائص الحروب الالكترونية ، واثبت بان المخاطر العالية التصنيف لا تحتاج الى جهود بشرية كبيرة ، بقدر حاجتها إلى خطط عسكرية مدروسة بشكل دقيق .

المحور الثاني :- الذكاء الاصطناعي .. المرونة في التوظيف العسكري .

تشهد البيئة الأمنية العامة تغيرا جذريا على رغم بقاء طبيعة الصراع على حالها ، ولا شك إن الذكاء الاصطناعي ما هو إلا المرحلة الأحدث من مراحل التطور العلمي والتكنولوجي التي توصل لها العقل البشري في إطار بحثه المستمر عن التفوق ، وتذليل معوقات الطبيعة ، ورفع قدراته التنافسية ، وزيادة إنتاجه ، وتحقيق الأمن والرفاهية عبر تدني التكاليف وتعظيم العوائد . [١٤]

إن الذكاء الاصطناعي هو جزء أساس من سلسلة الضربات القاتلة في السياق العسكري، ويشير إلى سلسلة من الخطوات المختلفة المؤدية إلى ضربة ناجحة ضد هدف محدد ، مثل تحديد الأهداف، وتتبعها، وأخيرا ضربها، وتقييم فعالية العملية، ويتلقى الذكاء الاصطناعي المعلومات من مصادر عدة ، كبيانات الهاتف ،وصور

[١٣] . موسوعة مقاتل من الصحراء ، مصدر سابق ذكره .
[١٤]. سعد عبيد السعيدي : الذكاء الاصطناعي.. الميادين التطبيقية الأساسية ، كراسة إستراتيجية ، مركز حمورابي للبحوث والدراسات الإستراتيجية ، ع ٢٦ ، ٢٠٢٤ ، ص٥ .

الأقمار الصناعية، ثم ينفذ خطوات فردية، ويستخلص استنتاجاته الخاصة . [١٥] ولقد أدت التطورات التكنولوجية، خاصة في مجالات الذكاء الاصطناعي والتصنيع فضلا عن الطباعة ثلاثية الأبعاد، وتكنولوجيا النانو، إلى زيادة قدرة الفواعل المسلحة من غير الدول والأفراد العاديين على امتلاك الأدوات اللازمة لشن الحروب . [١٦]

وتتنوع استخدامات الذكاء الاصطناعي خلال الحروب ، وتشمل مجموعة واسعة من التطبيقات التي تسهم في تعزيز القدرات العسكرية وتحسين الأداء الاستراتيجي في فترة الحرب وما بعدها، إذ يعمل الذكاء الاصطناعي في الحرب كعامل تمكين تحليلي ومعطل ومضاعف للقوة ، مما يؤثر في الأمن الدولي ، وذلك من خلال تحويل ميزان الدفاع الهجومي نحو الهجوم، ولعل من أكثر تلك الاستخدامات شيوعا ، ما يلي :- [١٧]

١. تعزيز القدرات الاستخباراتية والمعلوماتية :-

يمكن توظيف تقنيات الذكاء الاصطناعي في عمليات التشخيص والتحليل الاستراتيجي من خلال تحليل البيانات الضخمة لفهم الأنماط والاتجاهات العسكرية، وتطوير قدرات الاستطلاع والاستشعار عن بعد من خلال جمع المعلومات والبيانات من البر والبحر والجو، وكذلك تطوير قدرات التشفير والأمان السيبراني ، مما يحمي البيانات والمعلومات الحساسة من الاختراق .

---

١٥. الذكاء الاصطناعي وتأثيره على الحروب الحديثة: حرب غزة وأوكرانيا نموذجًا المركز الأوربي لدراسات مكافحة الإرهاب والاستخبارات ، ٦/ ١٠/ ٢٠٢٥ ، المكتبة الالكترونية :- https://www.europarabct.com/

16 . T. X. Hammes: Technologies converge and power diffuses: The evolution of small, smart, andcheap weapons, Policy Analysis (Cato Institute), no. 786, January 27, 2016, p. 1, 5 .

١٧. كيف يدير الذكاء الاصطناعي دفة الحروب الحديثة؟ دراسة منشورة ، مركز المستقبل للأبحاث والدراسات المتقدمة ، ٢٠/ ٥/ ٢٠٢٤ ، المكتبة الالكترونية :- https://futureuae.com/ar-AE/Mainpage/Item/9281/ai-militarization

٢. قياسات الرأي العام نحو الحرب:-

يستخدم الذكاء الاصطناعي لمراقبة وتحليل منصات التواصل الاجتماعي لفهم آراء ومشاعر الجمهور تجاه الحرب والأحداث ذات الصلة، فيما يمكن أن يستخدم في تحليل النصوص والمقالات الإخبارية والصور والفيديوهات المتعلقة بالحرب واستخلاص المعلومات الرئيسة وأبرز الاتجاهات منها ، مما يساعد على فهم تأثير الأحداث العسكرية على الرأي العام، وتحليل البيانات التاريخية للحروب والصراعات السابقة، واستخلاص دروس وتوقعات حول كيفية تطور ردود الأفعال العامة في حالات مماثلة في المستقبل .

٣. تقييم المخاطر واتخاذ القرارات:-

يستخدم الذكاء الاصطناعي في تحليل المخاطر، وتقدير الأضرار المحتملة للقرارات العسكرية ، مما يساعد على اتخاذ القرارات الإستراتيجية بناءا على معرفة أكبر بالتأثيرات المحتملة لأي من هذه القرارات .

٤. المشاركة في العمليات الميدانية والقتالية:-

يتم استخدام الذكاء الاصطناعي في تطوير وتحسين أنظمة الأسلحة الموجهة مثل: الطائرات من دون طيار والصواريخ الذكية، مما يزيد من دقتها وفاعليتها ، ويقلل من الخسائر البشرية والمدنية، ويستخدم أيضا في عمليات تحديد الأهداف وتصنيف المقاتلين، ويسهم في تحسين عمليات التواصل والتنسيق بين القوات المختلفة ، مما يزيد من فعالية العمليات العسكرية ويقلل من الفوضى والارتباك، فضلا عن تطوير الروبوتات القاتلة والأسلحة ذاتية التشغيل التي قد تشارك في العمليات القتالية الميدانية، وكذلك توظيف الذخائر ذاتية التحكم في العمليات العسكرية الدقيقة .

٥. جهود إعادة الإعمار في مرحلة ما بعد الحرب:-

يساهم الذكاء الاصطناعي في جهود تحقيق الاستقرار بعد الحرب، إذ يسهم في تقييم الأضرار وتحديد الأولويات في عمليات إعادة الإعمار من خلال تحليل صور وفيديوهات الأضرار الناجمة عن الحرب، وكذلك تعزيز جهود تنسيق العمليات الإنسانية عبر تحليل البيانات المتعلقة بالنازحين واللاجئين، وتحديد احتياجاتهم، وتعزيز الإصلاحات والمصالحة، من خلال تحليل البيانات السياسية والاجتماعية لتقديم التوجيهات والمقترحات لعمليات المصالحة بين الأطراف المتنازعة .

وفي رأيي المتواضع ، فاني أجد أن التضليل المعلوماتي المقصود هو مبدأ محوري في الاستراتيجيات الخاصة بالأمن القومي في الوقت الحاضر، يعيد تعريف التصورات والتوازنات العالمية ، وأنها تهدف إلى زعزعة الاستقرار ونشر الفوضى في عالم تتلاشى فيه الحدود بين الدول ويظهر الصراع المادي والرقمي بصورة أوضح .

ورغم التطورات الهائلة في مجال الذكاء الاصطناعي، والتوسع في استخدامه أثناء الحروب المعاصرة ، فلا تزال هناك بعض المخاطر والتبعات الناجمة عن هذا التوظيف في وقت الحرب، ومنها :- [١٨]

١. انتهاكات حقوقية:-

قد يواجه استخدام الذكاء الاصطناعي في الحروب تحديات أخلاقية وقانونية، خاصة فيما يتعلق بالقضايا المتعلقة بالقتل الآلي وحقوق الإنسان، إذ قد يتسبب

[١٨] . رماح الدلقموني : مستقبل الذكاء الاصطناعي.. ما هي أسوأ مخاطره المحتملة؟ وكيف نتصدى لها؟ دراسة منشورة ، قناة الجزيرة ، ٢٠٢٣/٦/١١ ، المكتبة الالكترونية :- https://www.aljazeera.net/tech

الاعتماد المفرط على التكنولوجيا في ارتكاب أخطاء قاتلة أو في مسائل تتعارض مع القوانين الدولية الإنسانية .

٢. **عدم الاعتمادية والثقة الكافية:-**

قد تواجه التطبيقات العسكرية للذكاء الاصطناعي تحديات فيما يتعلق بالاعتمادية والثقة ، إذ قد تواجه مشكلات تقنية تؤدي إلى عطل في الأنظمة أو تحول دون أداء مهامها المخططة .

٣. **الضرر العرضي:-**

مثل وقوع أخطاء فنية أو ضرر عرضي، خاصة في حالة استخدام الأسلحة المتحكمة بشكل آلي دون وجود رقابة بشرية كافية، وهو ما قد ينتج عنه قتل للمدنيين والأبرياء، ولاسيما في حالة الأخطاء المتكررة في تحديد الأهداف العسكرية والمسلحة، أو تدمير بنية تحتية وخدمية حيوية لا ترتبط بنشاط عسكري .

٤. **الخروج عن السيطرة:-**

قد يكون التفاعل بين أنظمة الذكاء الاصطناعي والقادة البشريين غير فعال، مما يؤدي إلى سوء التفاهم أو اتخاذ قرارات غير فعالة، وقد ينتج عنه تطبيق قرارات آلية دون تدخل بشري ، مما يثير مخاوف بشأن فقدان السيطرة الإنسانية على الآلة، وما قد ينتج عنه من سلوكيات ضارة بالمجتمعات .

٥. **تعزيز الاضطرابات الدولية والصراعات:-**

قد يزيد استخدام الذكاء الاصطناعي في الحروب من الفجوة بين الدول المتقدمة تقنيا، وتلك التي تفتقر إلى القدرات المتطورة ، مما يزيد من عدم المساواة ويعزز الاضطرابات الدولية .

٦. **تضاعف عدد القتلى من المدنيين:-**

أن توظيف أسلحة الذكاء الاصطناعي يؤدي إلى وقوع عشرات الآلاف من المدنيين الأبرياء، إذ إن استهداف شخص ما يحتمل أنه عسكري بناء على توصية

من برامج التحقق الذكية، قد يترتب عليه مقتل العشرات من المحيطين به دون تمييز، وهو ما يثير العديد من التبعات القانونية والأخلاقية بشكل عام إزاء العمليات العسكرية .

٧. عدم القدرة على حسم المعركة :-

رغم توظيف كافة القدرات الممكنة مثل: الأسلحة والذخائر الموجهة والطائرات من دون طيار وأدوات الاستشعار، زاد توظيف تلك التقنيات من تحقيق ما قد يكون إبادة جماعية ضد المواطنين وزيادة أعداد القتلى وتدمير البنية التحتية ، في حالتي غزة وأوكرانيا .

يمكن الإشارة إلى تطبيق لأنظمة الذكاء الاصطناعي بشكل عملي في الحروب على النحو التالي:- [١٩]

١. الحرب الأوكرانية :-

تعتمد أوكرانيا، بشكل متزايد على الذكاء الاصطناعي لتحقيق قدر من التفوق الميداني، إذ تسعى للتفوق في مجال الاستخبارات الجغرافية المكانية، إذ تستخدم أوكرانيا برنامج شركة Palantir لتحليل صور الأقمار الاصطناعية، والبيانات مفتوحة المصدر، ولقطات الطائرات من دون طيار، والتقارير من الأرض لتزويد القادة بالخيارات العسكرية، وهو البرنامج المسؤول عن معظم الاستهدافات في أوكرانيا ، وكما استخدمت أوكرانيا بيانات الشركة في مشروعات تتجاوز بكثير الاستخبارات في ساحة المعركة، بما في ذلك جمع الأدلة على جرائم الحرب، وإزالة الألغام الأرضية، وإعادة توطين اللاجئين النازحين، كما أسهمت شركات التكنولوجيا الرئيسة مثل: مايكروسوفت، وأمازون، وغوغل، وستارلينك في حماية أوكرانيا من الهجمات الإلكترونية الروسية، وترحيل البيانات الحكومية المهمة إلى الخوادم

[١٩] . كيف يدير الذكاء الاصطناعي دفة الحروب الحديثة ، مصدر سبق ذكره .

السحابية للحفاظ عليها، وإبقاء البلاد على اتصال، وفي المقابل ، نشرت روسيا الاتحادية ذخيرة من نوع كلاشينكوف ZALA Aero KUB-BLA التي تعمل بالذكاء الاصطناعي، في حين استخدمت أوكرانيا طائرات من دون طيار من طراز Bayraktar TB2 تركية الصنع، والتي تتمتع ببعض القدرات المستقلة .

٢. حرب غزة :-

أشارت تقديرات متعددة إلى أن إسرائيل سعت إلى أتمتة حربها الدائرة على غزة ، إذ تستخدم نظام ذكاء اصطناعي يطلق عليه اسم لافندر في عملياتها العسكرية داخل غزة، وهو نظام يقوم على تحديد الأهداف المحتملة، فقد شارك لافندر في تحديد ٣٧ ألف هدف خلال الأسابيع الأولى من الحرب، ويستكمل البرنامج برنامجين آخرين هما: أين هو أبي؟ والذي يستخدم لتعقب الأفراد الذين تم تحديدهم كأهداف وقصفهم عندما يكونون في المنزل، وبرنامج الإنجيل، الذي يهدف إلى تحديد المباني والهياكل .

ولا يفوتنا أن نذكر أن العدوان الأمريكي – الإسرائيلي الحاصل حاليا ضد الجمهورية الإسلامية الإيرانية قد استخدم الذكاء الاصطناعي بشكل مفرط من خلال متابعة الأهداف الحيوية ، والارتباط بالأقمار الصناعية ، وشبكات التجسس.

المحور الثالث :- الاستراتيجيات المعاصرة للأمن القومي وأدوات المواجهة المستقبلية .

تتفق معظم الأدبيات التي قامت بتعريف مفهوم الأمن على أنه يشير عموما إلى تحقيق حالة من انعدام الشعور بالخوف، وإحلال شعور الأمان ببعديه النفسي والجسدي محله، والشعور بالأمان كقيمة إنسانية كونية مرغوبة لا تقتصر على فئة اجتماعية معينة أو مرتبطة بمستوى الدخل، فالفقير مثل الغني يحتاج إلى الشعور بالأمان ويسعى إلى تحقيقه وإن اختلفت درجات المتمتع به، ونظرا لصعوبة تحقيق

الأمان الكامل، فقد أصبح ينظر للأمن على أنه مسألة نسبية مرهونة بالسعي لتعزيز أفضل الشروط لتوافره .

يعد الشعور بالأمن من النعم العظيمة التي منحها الله للإنسان، لأنه يهدف إلى تحقيق الأمن المجتمعي والنفسي والسكينة والاطمئنان التي يحتاجها ، لكي يزول عنه هاجس الخوف، ويشعر بالرضا والسعادة ، وجعل الله عز وجل من فقدان هذه النعمة نقمة، ينتقم بها الله من الخلق الفاسدين، والعاصين، والكافرين ، وبالتالي جاء مفهوم الأمن في القرآن الكريم ، لغرض التعبير عن طمأنينة النفس وزوال الهم والخوف ، والأمن يتعلق بالمستقبل، إذ يكون في مقابله خوف العدو ، ولذا عرفه بعضهم ، بأنه يتأتى من عدم توقع أي مكروه في الزمان المستقبلي .[٢٠] ولقد ورد كلمة الأمن في نص القرآن الكريم في موضعين، هما: { فأي الفريقين ،أحق بالأمن ، إن كنتم تعلمون ، الذين آمنوا، ولم يلبسوا إيمانهم بظلم، أولئك لهم الأمن وهم مهتدون }.[٢١]

والأمن في اللغة :هو بالضد من الخوف، ويشتق من أصل الفعل العربي أمِن ، أمْنا وأمَانًا ، فالأمن في لغة العرب: هو الطمأنينة الحاصلة للنفس، وذهاب الخوف منها ، ويقال: في الرجل أمنة ، أي أنه يأمن كل إنسان ، وقيل: يأمَنُه الناس، ولا يخافون غائلته ، ورجل أمَنةٌ أيضا، إذا كان يطمئن ، ويثق بكل إنسان .[٢٢] وقد ورد المفهوم في القرآن الكريم بقوله تعالى: "فليعبدوا رب هذا البيت الذي أطعمهم من جوع وآمنهم من خوف" .[٢٣]

أما مفهوم الأمن من الناحية الاصطلاحية: فهو يعني حالة الطمأنينة، وسكون القلب، ويقال: أمِن فلان منٌ الأسدَ أمْنًا، مثل: سَلِمَ منه، والأصل أن يستخدم في

---

٢٠ . محمد بن سليمان الواصل : الأمن في القرآن الكريم ، المعهد العلمي ، جامعة الإمام محمد بن سعود الإسلامية ، السعودية ، المكتبة الالكترونية :- https://units.imamu.edu.sa/shis/malaz-inst/EduArticles/Pages/14-2-1440-m.aspx

٢١ . القران الكريم : سورة الأنعام ، الآية ٨١- ٨٢ .

٢٢ . نقلا عن : محمد بن مكرم بن منظور الأفريقي المصري ، لسان العرب .

٢٣ . القران الكريم : سورة قريش، الآيتان ٣-٤.

سكون القلب، وأمِنَ البلدُ: اطمأنَّ به أهلُه، فهو آمِنٌ وأمينٌ، وهو مَأمُون الغائلة، أي ليس له مكر يخشى منه . [٢٤]

وقد عرفه قاموس بنغوين للعلاقات الدولية، بأنه مصطلح يشير إلى غياب ما يهدد القيم النادرة .[٢٥] أي أن الأمن هو مجموعة القواعد والقوانين التي يضعها مسؤول الأمن ، والتي يجب أن يتقيد ويلتزم بها جميع الأشخاص، الذين يتعاملون معه ، وهو مفهوم واسع جدا ، يشمل جميع عمليات التدخل ، والبقاء ، والتصرف في موقع ما ، ويشمل كذلك الأمن السيبراني، أمن جميع المواقع المهمة، وقواعد وأصول ضبط الاتصالات ، والأنظمة الالكترونية، ونقل المعلومات، وخزنها، والمحافظة عليها ، وعمليات استثمارها. [٢٦]

أما مفهوم الأمن القومي ، فيعني أشياء مختلفة لأشخاص مختلفين، فتقليديا كان يتم تعريف الأمن القومي على أنه الحماية من الهجوم الخارجي، وبالتالي فقد تم النظر إليه بشكل أساس على أنه يعني دفاعات عسكرية في مواجهة تهديدات عسكرية، وقد ثبت أن هذه الرؤية ضيقة جيدا، فالأمن القومي يتضمن ما هو أكثر من تجهيز قوات مسلحة واستخدامها ، والأكثر من ذلك، فإن مثل تلك الرؤية قد تجعل المرء يعتقد بأن أفضل طريق لزيادة الأمن هو زيادة القوة العسكرية ، وعلى الرغم من أن القوة العسكرية هي مكون مهم جداً في الأمن، فإنها تعد جانبا واحدا من جوانب الأمن، فالتاريخ ملئ في واقع الأمر بأمثلة لسباقات تسلح تسببت في إضعاف الأمن وليس في تقويته، تبدأ مثل هذه السباقات عادة بقيام دولة بتقوية

---

[٢٤] . عبد الكريم بن محمد الطاهر حامدي: مقصد حفظ الأمن في القرآن الكريم ، مجموعة بحوث ، مؤسسة الفرقان للتراث الإسلامي ، لندن ، بريطانيا ، ٢٠١٦ .

[٢٥] . ينظر في : إيفانز غراهام و نوينهام جيفري : قاموس بنغوين للعلاقات الدولية ، ترجمة : مركز الخليج للأبحاث ، الإمارات العربية المتحدة ، مركز الخليج للأبحاث ، ٢٠٠٤ .

[26] .Barbara Y. Fraser : Security handbook, RFC 2196, ,21\1\2021, https://datatracker.ietf.org/doc/rfc2196 .

**أرنولد ولفرز:- وهو محامي واقتصادي ومؤرخ وباحث في العلاقات الدولية من أصل أمريكي سويسري، اشتهر لعمله في جامعة ييل ولكونه رائدا في الواقعية الكلاسيكية في العلاقات الدولية .

قوتها العسكرية لأغراض دفاعية من أجل أن تشعر أنها أكثر أمنا، ويؤدي هذا الفعل بالدول المجاورة إلى أن تشعر بأنها مهددة، وترد على ذلك بأن تزيد من قدراتها العسكرية، مما يجعل الدولة الأولى تشعر أنها أقل أمنا فيستمر السباق ، وأدى ذلك إلى بروز الحاجة إلى صياغة تعريف أوسع للأمن القومي يتضمن الأبعاد الاقتصادية والدبلوماسية والاجتماعية، فضلا عن البعد العسكري، وقد قدم **أرنولد ولفرز**** مثل هذا التعريف عندما قال: (يقيس الأمن بمعناه الموضوعي مدى غياب التهديدات الموجهة للقيم المكتسبة، ويشير بمعناه الذاتي إلى غياب الخوف من أن تتعرض تلك القيم إلى هجوم) .[٢٧]

واجد كباحثة، انه ورغم أن الأمن مرتبط مباشرة بالقيم التقليدية ، فإنه ليس قيمة في حد ذاته، وإنما يمكن اعتباره من الناحية السياسية فقط ، بأنه موقف يسمح لدولة أو قومية ما بالحفاظ على قيمها، وبالتالي فإن الأمن يكون هنا فعلا أكثر منه قولا ، ولذلك فإن الأمن يصبح تقييما مبنيا على مفاهيم لا تتعلق بالقوة والضعف لدى طرف ما ، وإنما بالقدرات والنوايا الخاصة بالتهديدات المدركة .

ويعرف الأمن القومي بأنه: ذلك الجزء من سياسة الحكومة الذي يستهدف خلق الظروف المواتية لحماية القيم الحيوية .[٢٨] ويعرفه هنري كيسنجر بأنه يعني : أية تصرفات يسعى المجتمع عن طريقها إلى حفظ حقه في البقاء . [٢٩] أما روبرت مكنمارا فيرى أن الأمن : هو التنمية، وبدون تنمية لا يمكن أن يوجد أمن، والدول التي لا تنمو في الواقع، لا يمكن ببساطة أن تظل آمنة . [٣٠]

---

27 .Arnold Wolfers, Discord and collaboration, Essays on International Politics (Baltimore: John Hopkins University Press, 1962), P.150.

28 .Frank Trager and Philip Kronenberg (eds.), National Security and American Society (Kansas: Kansas University Press, 1973), p35-36.

29 . Henry Kissinger, Nuclear Weapons and Foreign Policy (London: Wild Field and Nicholson, 1969), p 46.

30 .McNamara, The Essence of Security (New York: Harper Press, 1966), p149.

أبرز الاستراتيجيات المعاصرة للأمن القومي:- [٣١]

تتسم هذه الاستراتيجيات بكونها غير روتينية، إذ تهدف إلى تغيير السلوك الدولي وحماية المصالح في عصر يتسم بـ ما بعد العولمة وأولويات الاقتصاد الوطني .

١. **الأمن الشامل والتعاون الإقليمي :-**

تبني استراتيجيات تربط الأمن القومي بالتنمية البشرية والاقتصادية والسياسية، والاعتراف بأن أمن الدولة يعتمد على أمن محيطها الإقليمي.

٢. **الاستراتيجيات التكنولوجية والسيبرانية :-**

حماية الفضاء السيبراني، وشبكات المعلومات، والبنية التحتية الحيوية من الهجمات، إذ أصبحت التكنولوجيا مصدرا رئيسا للقوة .

٣. **أمن الموارد والطاقة :-**

التركيز على استدامة الإمدادات الغذائية، أمن الطاقة، ومواجهة تحديات التغير المناخي والتهديدات البيئية .

٤. **الاستثمار في القدرات الذاتية والردع :-**

تطوير القوة العسكرية والاقتصادية المباشرة، مع تعزيز مصداقية الردع لضمان حماية الحدود والمصالح الوطنية.

٥. **الشراكات والتحالفات الإستراتيجية :-**

تشكيل تحالفات لتعزيز النفوذ الجماعي ومواجهة التحديات العابرة للحدود مثل الإرهاب والجريمة المنظمة .

---

٣١. ريناس بنافي : المفهوم المعاصر للأمن القومي وإشكاليات المعضلة الأمنية، **المركز الديمقراطي العربي** ، بحث منشور ، ٢٠١٦/١٢/٢٥ ، المكتبة الالكترونية :- https://democraticac.de/?p=41634

الخـــــاتمة .

أصبح الفضاء الإلكتروني عنصرا مؤثرا في النظام العالمي ، نظرا لما يحمله من أدوات تكنولوجية متطورة تؤدي دورا مهما في عمليات الحشد والتعبئة في العالم برمته ، فضلا عن التأثير في القيم السياسية والتأثير على أنماط القوة ، والحرب ، والأمن ، وتستخدم العديد من الدول القدرات التي يوفرها الفضاء الإلكتروني لاعتبارات في مقدمتها الأمن والقوة العسكرية ، وهذا جعل تلك الدول تدخل الفضاء الإلكتروني ضمن حساباتها في إعادة صياغة مفاهيم الإستراتيجية وأمنها القومي ، وأصبحت الجيوش الالكترونية العسكرية في كافة أنحاء العالم ، تهتم بحرب المعلومات ودورها في حروب المستقبل ، وبما أن خصائص الحروب الالكترونية تتفوق على خصائص الدفاع التقليدية ، فان ذلك ما سيدفع العالم إلى مزيد من الصراعات وخاصة مع تطور آليات الهجوم الالكتروني بشكل متسارع ، فاستبدال الحرب العسكرية بتلك الالكترونية وانتقال الصراع ما بين القوى العظمى من المساحات التقليدية إلى الفضاء الالكتروني قد يسمح للقوى العالمية الدخول في مواجهات الكترونية تعيد تشكيل خرائط النفوذ العالمية ، وتفتح الباب أمام أنماط جديدة من التهديدات والفرص في وقت واحد ، ومع ذلك فهناك بعض النتائج التي توصلنا لها ، وهي :-

١. إن مفهوم الحرب الالكترونية يمكن أن يتوسع بشكل اكبر في المستقبل .

٢. إن العراق في موقف عسكري صعب لافتقاره إلى النظم المتقدمة الخاصة بالحروب الالكترونية .

٣. هناك ضرورة لاعتماد نظم للمعلومات والتقنيات في المؤسسات العسكرية لتحسين كفاءة وفاعلية أدائها .

٤. الحاجة لتطوير سياسات واستراتيجيات خاصة بالذكاء الاصطناعي ، بهدف تنمية مرافق الدولة ، وذلك لتحقيق نمو أكثر فاعلية .

المصـــــادر .

١. القران الكريم : سورة الأنعام ، الآيتان ٨١- ٨٢ .
٢. القران الكريم : سورة قريش، الآيتان ٣-٤.
٣. إبراهيم إسماعيل كاخيا : الحرب الالكترونية ، مجلة الدفاع العربي ، المكتبة الالكترونية :- http://www.arabdefencejournal.com
٤. أشرف صلاح الدين: الانترنت.. عالم متغير ، ط١، مركز الحضارة العربية ، القاهرة ، مصر ، ٢٠٠٣.
٥. الذكاء الاصطناعي وتأثيره على الحروب الحديثة: حرب غزة وأوكرانيا نموذجًا المركز الأوربي لدراسات مكافحة الإرهاب والاستخبارات ، ١٠/٦/ ٢٠٢٥ ، المكتبة الالكترونية :- https://www.europarabct.com/
٦. إيفانز غراهام و نوينهام جيفري : قاموس بنغوين للعلاقات الدولية ، ترجمة : مركز الخليج للأبحاث ، الإمارات العربية المتحدة ، مركز الخليج للأبحاث ، ٢٠٠٤ .
٧. جعفر جاسم :حرب المعلومات بين أرث الماضي وديناميكية المستقبل ، ط١ ، دار البداية للنشر والتوزيع ، عمان ، الأردن ، ٢٠١٠ .
٨. رماح الدلقموني : مستقبل الذكاء الاصطناعي.. ما هي أسوأ مخاطره المحتملة؟ وكيف نتصدى لها؟ دراسة منشورة ، قناة الجزيرة ، ٢٠٢٣/٦/١١ ، المكتبة الالكترونية :- https://www.aljazeera.net/tech
٩. ريناس بنافي : المفهوم المعاصر للأمن القومي وإشكاليات المعضلة الأمنية، المركز الديمقراطي العربي ، بحث منشور ، ٢٠١٦/١٢/٢٥ ، المكتبة الالكترونية :- https://democraticac.de/?p=41634
١٠. سعد عبيد السعيدي : الذكاء الاصطناعي.. الميادين التطبيقية الأساسية ، كراسة إستراتيجية ، مركز حمورابي للبحوث والدراسات الإستراتيجية ، ع ٢٦ ، ٢٠٢٤ .
١١. صفات سلامة : أسلحة حروب المستقبل بين الخيال والواقع ، مركز الإمارات للدراسات والبحوث الإستراتيجية ، ط١، أبو ظبي ، الإمارات العربية المتحدة ، ٢٠٠٥ .
١٢. عباس بدران : الحرب الالكترونية .. الاشتباك في عالم المعلومات ، مركز دراسات الحكومة الالكترونية للنشر والتوزيع ، بيروت ، ٢٠١٠ .
١٣. عبد الكريم بن محمد الطاهر حامدي: مقصد حفظ الأمن في القرآن الكريم ، مجموعة بحوث ، مؤسسة الفرقان للتراث الإسلامي ، لندن ، بريطانيا ، ٢٠١٦ .
١٤. عبد الكريم صالح المحسن : ساحة المعارك العظمى التالية : الفضاء الالكترونية ، الحوار المتمدن ، محور الأبحاث السياسية ، ع ٣٦٠٤ ، ٢٠١٢ ، المكتبة الالكترونية :- https://www.ahewar.org/debat/shoe.art.asp
١٥. كمال السعدي : الحرب الالكترونية ، ط١ ، المركز العربي للدراسات الإستراتيجية ، المؤسسة العربية للدراسات والنشر ، بيروت ، لبنان ، ١٩٧٧ .
١٦. كمال مساعد : الحرب الافتراضية وسيناريوهات محاكاة الواقع ، مجلة الجيش اللبناني ، ع ٢٥٣، ٢٠٠٦ ، المكتبة الالكترونية :- https://www.leparmy.gov.Ib/artical.asp
١٧. . كيف يدير الذكاء الاصطناعي دفة الحروب الحديثة؟ دراسة منشورة ، مركز المستقبل للأبحاث والدراسات المتقدمة ، ٢٠٢٤/٥/٢٠ ، المكتبة الالكترونية :- https://futureuae.com/ar-AE/Mainpage/Item/9281/ai-militarization

١٨. محمد بن سليمان الواصل : الأمن في القرآن الكريم ، المعهد العلمي ، جامعة الإمام محمد بن سعود الإسلامية ، السعودية ، المكتبة الالكترونية :- https://units.imamu.edu.sa/shis/malaz-inst/EduArticles/Pages/14-2-1440-m.aspx
١٩. محمد بن مكرم بن منظور الأفريقي المصري ، لسان العرب .
٢٠. موسوعة مقاتل من الصحراء ، المكتبة الالكترونية :- http://www.moqatel.com
٢١. وليد غسان سعيد جلعوط : دور الحروب الالكترونية في الصراع العربي الإسرائيلي ، رسالة ماجستير غير منشورة ، جامعة النجاح الوطنية ، فلسطين ، ٢٠١٣ .
22. Arnold Wolfers, Discord and collaboration, Essays on International Politics (Baltimore: John Hopkins University Press, 1962) .
23. Barbara Y. Fraser : Security handbook, RFC 2196, ,21\1\2021, https://datatracker.ietf.org/doc/rfc2196
24. Frank Trager and Philip Kronenberg (eds.), National Security and American Society (Kansas: Kansas University Press, 1973) .
25. Henry Kissinger, Nuclear Weapons and Foreign Policy (London: Wild Field and Nicholson, 1969) .
26. Johan M.G. van der Dennen, On War: Concepts, Definitions, Research Data - A Short Literature Review and Bibliography, University of Groningen, 2005, https://bit.ly/2VvgDWl
27. McNamara, The Essence of Security (New York: Harper Press, 1966) .
28. T. X. Hammes: Technologies converge and power diffuses: The evolution of
small, smart, and cheap weapons, Policy Analysis (Cato Institute), no. 786, January 27, 2016 .