التهديدات الأمنية الهجين في العلاقات الدولية (السيبرانية والذكاء الاصطناعي نموذجاً)

د.سوزي رشاد

أستاذ مساعد– قسم العلوم السياسية– جامعة ٦ أكتوبر

ملخص الدراسة:

أثرت الثورة التكنولوجية بشكل كبير في حقل العلاقات الدولية خاصة مع تطور المجال السيبراني وتقنيات الذكاء الاصطناعي اللذان يمثلان موجات من استخدام التطور التكنولوجي في قضايا السياسة الدولية، وقد كان لهذا التطور تأثير في ظهور نوع جديد من التهديدات الأمنية أطلق عليها "التهديدات الهجين" التي تتضمن مجموعة متنوعة من القدرات التقليدية والغير تقليدية في ساحة المعركة العملياتية، أثرت على مصادر القوة ووسائلها على الساحة الدولية مع ظهور مفاهيم جديدة معتمدة على الفضاء التكنولوجي والتقني، بالاضافة إلى التغير في أنماط الصراع والحروب وظهور فواعل جديدة مؤثرة، وبالتالي آثارت الورقة البحثية تساؤل رئيسي حول طبيعة التهديدات الأمنية الجديدة وأثرها في العلاقات الدولية من خلال دراسة نموذجين لتلك التهديدات وهما السيبرانية والذكاء الاصطناعي، وخلصت الدراسة إلى أن تلك النماذج كان لها تأثير على مستوى التفاعلات ومستوى المفاهيم في حقل العلاقات الدولية من حيث تطور مفهوم القوة والأمن والحرب والصراع وأدواتهم.

الكلمات المفتاحية: التهديدات الهجين، السيبرانية، الذكاء الاصطناعي، سباق التسلح التقني، عسكرة الفضاء، القوة الناعمة، العلاقات الدولية.

Abstract:

The technology revolution has greatly affected the field of international relations, especially with the development of the cyber field and artificial intelligence techniques, which represent waves of the use of technological development in

(ISSN: 2536 - 9555)

international issues, and this development has had an impact on the emergence of a new type of security threats called "hybrid threats" that include a variety of And the dynamics of traditional and unconventional capabilities in the operational battlefield, which affected the sources of power and their means on the international scene with the emergence of new concepts based on technological and technical space, in addition to the change in patterns of conflict and wars and the emergence of new influential actors, and thus the research paper raised a major question about the nature of threats The new security and its impact on international relations by studying two models of those threats, namely cyber and artificial intelligence, and The study concluded that those models had an impact on the level of interactions and the level of concepts in the field of international relations in terms of the development of the concept of power, security, war and conflict and their tools. .

مقدمة:

مرت البشرية بالعديد من الثورات التي أثرت على جميع جوانب الحياة بداية من الثورة الصناعية الأولى إلى الثورة الصناعية الرابعة التي ارتبطت بالتكنولوجيا وتقنيات الذكاء الاصطناعي، وقد أدت الثورة التكنولوجية إلى حدوث طفرة في بروز أهمية التكنولوجيا والعلم في الحياة السياسية، وتناولت العديد من الدراسات بداية فترة التسعينات قضايا التكنولوجيا والسياسة وظهر تيار أطلق عليه دراسات التكنولوجيا والعلم Science and Technology Studies (STS)، والذي اهتم بتأثير العلم والتكنولوجيا على جميع التخصصات بما في ذلك تخصص العلوم السياسية.

وقد أثرت الطفرة التكنولوجية على طبيعة أنشطة وأدوات وإدارة القضايا السياسية، وتبلور ذلك في تطورين مهمين على المستوى الالكتروني وهو المجال السيبراني والذكاء الاصطناعي، اللذان أفرزا في المقابل قضايا جديدة غير تقليدية

على الساحة الدولية تطلب معها أدوات مختلفة في التعامل، والاعتراف بفواعل متعددة جديدة في المجال الدولي لها تأثير في توجيه القضايا الدولية، مما أنتج معها تهديدات أمنية جديدة في العلاقات الدولية أطلق عليها العديد من المصطلحات منها التهديدات غير التقليدية أو التهديدات اللاتماثلية أو التهديدات الهجين في العلاقات الدولية.

وقد استفادت الدول والحكومات بشكل فعال من الفضاء الالكتروني في الأنشطة المتفرقة جغرافيا التي يكون تنفيذها أكثر صعوبة في المجال المادي، وفي الواقع يرتبط الأمن السيبراني بالذكاء الاصطناعي، حيث أن الأخير سيكون له آثار تحويلية على الحرب الألكترونية والأمن السيبراني بصفة عامة، فسيقلل الذكاء الاصطناعي والتعلم الآلي من عدد البشر اللازمين لأداء مهام محددة في المجال السيبراني، كما سيؤدي الاعتماد المتزايد للذكاء الاصطناعي في المجال السيبراني إلى زيادة قوة الأفراد الذين يقومون بتشغيل هذه الأدوات والأنظمة والإشراف عليها. وسيكون الذكاء الاصطناعي مفيدًا في تعزيز الدفاع السيبراني، فيمكن تحسين البحث عن نقاط الضعف وأنظمة المراقبة باستخدام الأتمتة الذكية، كما سيمكن الذكاء الاصطناعي من اضافة نماذج جديدة للدفاع السيبراني، حيث تعتمد معظم أنظمة الدفاع السيبراني اليوم على افتراضات معرفة مسبقة، وبالتالي قد يسمح الذكاء الاصطناعي والتعلم الآلي للأنظمة ليس فقط بالتعلم من نقاط الضعف السابقة، ولكن أيضًا بمراقبة السلوك الشاذ لاكتشاف التهديدات غير المعروفة والاستجابة لها، ولهذا يعد استخدام الذكاء الاصطناعي في مجال العلاقات الدولية الموجة الثانية من استخدام الفضاء الالكتروني والمجال السيبراني في الساحة الدولية، فهو مرحلة من مراحل التطور التكنولوجي على الساحة الدولية.

إشكالية الدراسة:

أصبحت الهجمات الالكترونية مصدر قلق في العلاقات الدولية لما لها من طبيعة مختلفة عن الهجمات التقليدية خاصة مع التطور التكنولوجي السريع في المجال السيبراني وتقنيات الذكاء الاصطناعي، ومن هنا حاولت الدراسة رصد

(ISSN: 2536 - 9555)

طبيعة تلك الهجمات وأثرها على العلاقات الدولية من خلال الاجابة على السؤال التالي "**ما هي طبيعة التهديدات الأمنية الجديدة وما أثرها في العلاقات الدولية؟ وذلك بالتركيز على السيبرانية والذكاء الاصطناعي كنماذج لتلك التهديدات**".

ومن السؤال الرئيسي تتفرع بعض الأسئلة وهي:

١. ماذا تعني التهديدات الهجين؟
٢. ما هي خصائص تلك التهديدات وطبيعتها؟
٣. كيف أثرت السيبرانية والذكاء الاصطناعي على طبيعة التفاعلات والمفاهيم السائدة في العلاقات الدولية؟

منهج الدراسة:

تعتمد الدراسة على **المنهج الوصفي التحليلي** الذي يهدف إلى الاحاطة بالأبعاد الواقعية للظواهر من خلال تحديد تلك الظواهر المراد بحثها وجمع المعلومات وفحصها ودراستها وتحليلها وصياغة النتائج، وهذا ما تعتمد عليه الورقة البحثية في دراسة السيبرانية والذكاء الاصطناعي كنموذج للتهديدات الهجين في العلاقات الدولية ورصد تأثيراتهما على تفاعلات وأدوات ومفاهيم العلاقات الدولية.

أهمية الدراسة:

تنبع أهمية الدراسة من محاولة الوقوف على طبيعة وتأثير التهديدات الجديدة في العلاقات الدولية واستشراف مستقبل تلك التهديدات من خلال تقديم نموذجين من التهديدات يمثلان انعكاس لظاهرة التطور التكنولوجي واستغلاله في الساحة الدولية وهما السيبرانية والذكاء الاصطناعي.

تقسيم الدراسة:

تنقسم الدراسة إلى ثلاثة محاور؛ يتناول المحور الأول مفهوم التهديدات الأمنية الهجين في العلاقات الدولية وملامحها وخصائصها، أما المحور الثاني فيتناول نموذج التهديدات السيبرانية من حيث مفهومها وملامح تأثيرها على العلاقات الدولية، كما يناقش المحور الثالث مفهوم الذكاء الاصطناعي والآثار المتوقعة له في العلاقات الدولية.

المراجعات الأدبية:

يمكن تقسيم الأدبيات الخاصة بالتهديدات الهجين إلى أربع مدارس فكرية مختلفة **أولها** مايطلق عليه "مكافحة التمرد" The Counterinsurgents يتحدى أنصار هذا التوجه الاتجاه الضيق للقوى المركزة تقليديًا ويدعون إلى تحول قائم بناء على طبيعة معارك اليوم. وهم يعتقدون أن العراق وأفغانستان يمثلان نقطة فاصلة في طبيعة تطور شكل الصراع. يؤكد مؤيدوا هذا الاتجاه أن التشكيلات الحاشدة المكونة من أسلحة تقليدية ونزاع واسع النطاق بين القوى التقليدية ليست سيناريوهات تخطيط واقعية ولا ينبغي أن تكون نقطة محورية لتشكيل جيش الغد، وأن الاستعداد للتهديدات غير التقليدية ضروري لتأمين مصالح الدولة، ومن مناصري هذا الاتجاه الكاتب Bastian Giegerich الذي أكد في مقالته "الحرب الهجين: وتغيير ملامح الصراع" على أن الصراعات الهجينة تتحدى الأشكال التقليدية للحرب والسلام، وأن مفاهيم الحرب المختلطة أصبحت عنصرا أساسيا في السياسات الدفاعية والأمنية، وأن الصراع الدولي سوف يشهد مزيد من الهجينة، وبالتالي يجب استعداد الدول لمواجهة التهديدات المختلطة بطرق غير تقليدية تتسم بالمرونة، كما يؤكد أن نظرية الحرب الهجينة تعد نهجًا جديدًا يمكن للدول أو مجموعات الجهات الفاعلة غير الحكومية من خلالها الوصول إلى مصالحها وأهدافها الاستراتيجية من خلال مزج مجموعة متنوعة من التكتيكات والتقنيات بطريقة أصلية لتحطيم القوات المسلحة الغربية الحديثة من خلال المزج بين أنماط ومستويات الحرب، واستخدام التكتيكات والتقنيات الهجينة للحصول على تأثيرات استراتيجية وتحقيق أهداف سياسية(١).

أما **الاتجاه التقليدي** The Traditionalists فينطلق من فرضية مؤداها أن الصراعات ستكون تقليدية وعالية الكثافة بشكل أساسي، مع عدم تجاهل الحروب غير النظامية، إلا أنهم يروا أن تلك الحروب هي حالات طارئة لا ينبغي أن تكون محور الجيوش القوية مثل الجيش الأمريكي، وبالتالي يجب إعادة تركيز القوات المسلحة على "القتال والفوز في حروب الأمة". ويركز أنصار هذا الاتجاه على

(ISSN: 2536 - 9555)

الحروب الكبرى عالية الكثافة بين الدول، ويدافعون عن إعادة توجيه القوات، وتكوين جيشًا كبيرًا من الناحية الاستراتيجية، وقد أيد ذلك الاتجاه Volker Boege في مقالته "المناهج التقليدية لتحويل الصراع: الامكانيات والحدود"، حيث أكد أنه بالرغم من محدودية تطبيق المناهج التقليدية في الصراع في حالة المجتمعات المفككة إلا أنه من الخطأ تجاهل هذه الإمكانية وعدم الاستفادة منها حيثما أمكن ذلك. وأكد على أن الأساليب التقليدية قد تعطي رؤى أوسع لعمليات تحويل الصراع بشكل عام. وأنه بالرغم من أن حل النزاعات التقليدية بالتأكيد ليس الدواء الشافي لجميع المشاكل، إلا أنه نهج تم التقليل من شأنه، وأن النهج التقليدي لا يعني العودة إلى "العصور القديمة الجيدة" لحل النزاعات التقليدية، ولكنه طريقة للمضي قدمًا من أجل التوافق الإيجابي المتبادل بين المقاربات التقليدية من ناحية والمقاربات الحديثة من ناحية أخرى(٢). أما **المدرسة الثالثة** والأكثر انتشارًا، على الأقل بين قادة القوات البرية الأمريكية، هي مدرسة Utility Infielder، حيث يدرك المدافعون عنها الحاجة إلى التعامل بشكل مناسب مع كل من المهام التقليدية الصارمة والتهديدات غير النظامية. ويقترحون تغطية النطاق الكامل للنزاع وتجنب مخاطر التركيز على أي من الطرفين، ويؤكد هذا الاتجاه على أهمية العمليات الكاملة التي تركز على القوات التكيفية والمرنة القادرة على القتال والفوز في القتال من خلال التوازن بين المهمة التقليدية والتهديدات الجديدة، وهذا ما أكد عليه Frank Hoffman في مقالته "التهديدات المختلطة: ما بين القدرة المطلقة وقابلية القهر"، والتي تناولت الأهمية التي حظيت بها التهديدات الهجينة في دوائر السياسة الرسمية، وكيف أنها أثبتت قدرتها على استخدام التكتيكات الغير نظامية والقدرات المتطورة التقليدية بجانب الأنشطة الغير قانونية والارهابية، وأهمية التوازن بين استخدامها واستخدام الأسلحة التقليدية. أما مدرسة "تقسيم العمل" Division of Labor وهي **المدرسة الرابعة**، يجادل أنصارها بأن الحرب غير النظامية والتقليدية هي أنماط مختلفة بشكل ملحوظ للصراع تتطلب قوات مميزة مع تدريب ومعدات وتصاميم مختلفة للقوة، ويركز هذا

المعسكر بشكل كبير على منع الصراع، والاستعداد لعمليات الاستقرار، والاستثمار في أشكال غير مباشرة من القوات الأمنية بدرجة أكبر من التخصص في مهام التعاون الأمني والقتال، وقد قدم Charles Sammons في اطار هذا الاتجاه الفكري وصفه لعمل الجيش الأمريكي من خلال فكرة تقسيم العمل، حيث جادل في مقالته بعنوان "تقسيم جديد للعمل: مواجهة التحديات الأمنية لأمريكا خارج العراق"، أن تعزيز الاستقرار والديمقراطية في الخارج يتطلب عدد أقل من القوات البرية واستخدام طرق مختلفة، أما الحروب الإقليمية التي قد يُطلب من القوات الأمريكية خوضها– التي تشمل إيران والصين (على تايوان) وكوريا الشمالية– تتطلب التزامات كبيرة من القوات الجوية والبحرية التقليدية[٣].

المحور الأول

الإطار النظري والمفاهيمي "للتهديدات الهجين"

أولا: الإطار النظري.

تعتمد الدراسة في إطارها النظري على مقولات دايفيد ليون وديدي بيغو، المنتميان لمدرسة باريس للدراسات الأمنية، حيث يشير دايفيد ليون إلى ما أطلق عليه "المراقبة أو العين الالكترونية"، التي تعني أن السلطة يجب أن تكون منظورة وغير ملموسة، ولها أنشطة جديدة وتتخذ في مجتمعنا المعاصر أشكالا عديدة منها استخبارات الاتصالات، واستخبارات الرادار، والاستخبارات الالكترونيات، واستخبارات الصور، حيث تعمل جميعها تحت علامة الاستخبارات التقنية التي تشكل نظاما جديدا للقوة في العلاقات الدولية، وتعمل بمثابة مصدر تقني استراتيجي للحقيقة الأمنية، من خلال قدرتها الظاهرة على توفير المعلومات المفصلة الخالية من القيمة حول موضوع المراقبة معتمد على أن "الصورة لا تكذب"، أيضا مجموعة المقولات الخاصة بالتهديدات الأمنية الغير تقليدية التي ظهرت مع العولمة والتي تتداخل معها تحديات الأمن الداخلي والأمن الخارجي، مما أدى إلى زيادة حجم التأثيرات الأمنية وبالتالي

(ISSN: 2536 - 9555)

من أهمية التركيز على الوكالات الأمنية العبر وطنية، وتكوين شبكة تجسد الروابط بين مختلف المؤسسات الأمنية التي تتجاوز الحدود والتنسيق فيما بينها وهو الأمر الذي من شأنه أن يؤسس إلى مفهوم تكنو– استراتيجي قائم على تقنيات المراقبة كما وصفه ديدي بيغو(٤).

كما تعتمد الدراسة على فرضية جوزيف ناي في مقالته عن القوة الناعمة حيث أشار إلى أن التغييرات التي شهدها العالم بعد نهاية الحرب الباردة، وأهمها زيادة اتجاهات العولمة والتقدم التكنولوجي الاستثنائي الذي يمكن التعبير عنه بالثورة المعلوماتية سبب في الجزء الاعظم من المشكلات والتهديدات التي تنتاب العالم اليوم. ويوضح ناي أن هذه المتغيرات، وخاصة المتغير التكنولوجي، أدت الى تراجع التهديدات المرتبطة بالقوة الصلبة لصالح ظهور التهديدات المرتبطة بالقوة الناعمة، والتي خلقت تهديدات لا تتمتع فيها اي دولة بميزة مطلقة كونها تقع خارج سيطرة القوة العسكرية والبنى الأساسية الحكومية والسيطرة المؤسسية. ويضيف ناي قائلا "أن هذا النوع من التغيرات أدى الى خصخصة الحرب وما يرتبط بها من تهديدات فتحولت الحرب الى معارك أفراد ضد دول وليس دول ضد دول كما كانت في الماضي، ويخلص الى أن مواجهة هذه التهديدات الجديدة تحتاج الى وسائل جديدة، فإذا كان استخدام القوة العسكرية يمكن أن يحقق نتائج إيجابية في حالات محدودة من هذه التهديدات فأن المطلوب هو أشكال جديدة ومختلفة من القوة وفي مقدمتها القوة الناعمة"(٥).

ثانيا: الإطار المفاهيمي.

ظهر هذا المفهوم الجديد في الأساس ضمن منظور القوات الأمريكية حول كيفية التعامل مع البيئات العملياتية المعقدة حيث يستخدم الخصم طرق عملياتية غير مقيدة، ويجمع بين جميع الأدوات المتاحة لتحقيق الأهداف، وبالتالي يفسر الحالات الغير تقليدية التي تنشأ في حالات التهديد وليس لها توصيف معين بغض النظر عن الدلالات.

ففي عصر الصراع الحالي، أدركت القيادة الأمريكية العسكرية أن النزاعات في المستقبل لن يتم وصفها حصريًا في بنيات الحرب التقليدية أو غير النظامية فقط، بل سيستخدم الأعداء مجموعات من الأساليب التقليدية وغير النظامية والتخريبية من أجل تحقيق ميزة عملياتية واستراتيجية. لذلك يوفر بناء التهديد المختلط إطارًا لوصف الطابع المتطور للجهات الفاعلة في مجال التهديد المعاصر، وتحدي منهجيات تقييم التهديدات التقليدية وإبراز ديناميات بيئة العمليات المعاصرة.

وقد تم استخدام العديد من المصطلحات لوصف التهديدات الجديدة في العلاقات الدولية، حيث استخدمت بعض الدراسات مفهوم "التهديدات اللاتماثلية" Asymmetric threats، وكان أولها دراسة لماك أندرو بعنوان "لماذا تخسر الدول الكبرى الحروب الصغيرة: سياسات الصراع اللاتماثلي" عام ١٩٧٥ والذي أشار فيها أن حروب فيتنام والجزائر أظهرت أن التفوق العسكري التقليدي الساحق للدول الكبرى لا يضمن لها عدم الهزيمة ضد الدول الصغيرة وفقا لطبيعة الحرب، وتكلفتها، ومدتها، والعناصر التي تواجهها[٦]. بينما استخدمت مجموعة أخرى من الدراسات مصطلح "التهديدات غير التقليدية" Unconventional threats وكان أولها مقالة لريتشارد أولمان بعنوان "إعادة تعريف الأمن"[٧]، والذي حذر فيها من التركيز على التهديد العسكري فقط لأمن الدولة، وينطلق من الافتراض القائل بأن تعريف الأمن القومي من الناحية العسكرية فقط ينقل صورة خاطئة مضلله عن الواقع ويمثل خطورة لأنه أولاً، يتسبب في تركيز الدول على التهديدات العسكرية وتجاهل الأخطار الأخرى وربما الأكثر ضرراً، وبالتالي فإنه يقلل من أمنهم الكامل. وثانيًا، يساهم في انتشار عسكرة العلاقات الدولية التي لا يمكن أن تؤدي إلا إلى زيادة انعدام الأمن العالمي على المدى الطويل. وأكد على أن التهديدات أصبح لها طبيعة غير تقليدية تهدد الخيارات السياسية المتاحة للفواعل الدولية، أما مصطلح "التهديدات الهجين"، وهو المصطلح الذي تتبناه الدراسة، عبر في البداية عن الجماعات غير النظامية والجماعات الارهابية، والجريمة المنظمة، والهجرة غير الشرعية[٨].

(ISSN: 2536 - 9555)

ويعود استخدام كلمة "هجين Hybrid" إلى تحليل قامت به قوات سلاح البحرية الأمريكية للتجارب العملياتية في العراق وأفغانستان، ففي سنة ٢٠٠٥ كتب الجنرال "جيمس ماتيس James Mattis" الذي شغل منصب قائد القيادة المركزية الأمريكية عن ظهور طرق غير منتظمة للتهديدات مثل: الإرهاب وأعمال التمرد وتجارة المخدرات، وناقش ماتيس حاجة الجيش الأمريكي للتحول إلى قوة "مختلطة" توسع وسائلها غير التقليدية دون التضحية بكفاءة قتال الحربية الكلاسيكية[٩]، وفي مقال نشر عام ٢٠٠٨، وصف رئيس أركان الجيش الأمريكي التهديد المختلط بأنه خصم يتضمن "مجموعات ديناميكية ومتنوعة من القدرات التقليدية وغير التقليدية بالاضافة إلى الارهابية والاجرامية"، خصم يستخدم في وقت واحد وبشكل تكيفي مزيجًا مخصصًا من الوسائل أو الأنشطة التقليدية وغير النظامية والإرهابية والإجرامية في ساحة المعركة العملياتية[١٠].

وتعد كتابات فرانك هوفمان[١١]Frank Hoffman نقطة انطلاق تحليلية جيدة لتوضيح المفهوم، فقد كان هوفمان من بين الكتاب الذين صاغوا المصطلح في تجسده الحالي. وقد اعتمد في صياغة تعريفه على استراتيجية الدفاع الوطني الأمريكي لعام ٢٠٠٥ واستراتيجية المراجعة السريعة Quadrennial Defense Review(QDR) لعام ٢٠٠٦ التي تركز على أنماط الصراع لدى الخصم، وقد حددت تلك الوثيقة بشكل ملحوظ أربعة أنواع مميزة من المنافسين الذين كان على الجيش الأمريكي الاستعداد لهم؛ بما في ذلك التهديدات التقليدية traditional threats، والأعداء غير النظاميين irregular foes، والتهديدات الكارثية catastrophic threats، والمتحدون المزعجون disruptive challengers. وقد سعت الفئة الأخيرة إلى تحديد الاختراقات الثورية بعيدة المدى التي قد تشكل تحولات "تغيير قواعد اللعبة" في الأسلحة أو التكنولوجيا الجديدة التي من شأنها أن تعوض تمامًا المزايا الأمريكية اليوم. ويؤكد هوفمان على احتمالية ظهور مزيج من

التهديدات المختلفة ذات الطبيعة الغير تقليدية. ويعرف التهديدات الهجينة بأنها[١٢] **"تتضمن مجموعة كاملة من الوسائل المختلفة من الحرب بما في ذلك القدرات النظامية والتكتيكات والأشكال غير النظامية بالاضافة إلى الأعمال الإرهابية بما في ذلك والإكراه والعنف والإجرام العشوائي"**. وشدد هوفمان على أن التهديدات المختلطة تصل إلى ما هو أكثر بكثير من مجرد تركيبات بسيطة من مجموعة متنوعة من الجهات الفاعلة والتكتيكات والأساليب، حيث تولد التهديدات الهجين أنماطًا مختلفة من الصراع الذي يصعب التعامل معه، لأنه يخلط بين المفاهيم الغربية الثنائية للسلام والحرب، والوسائل العسكرية وغير العسكرية، والمقاربات التقليدية وغير النظامية. وجادل هوفمان بأن الجهات الفاعلة الغربية "تفكر في الأشياء بمصطلحات الأبيض والأسود" ولا تزال بحاجة إلى تحسين كبير في فهم الصراع في المساحات الواقعة بينهما في المناطق الرمادية. ونظرًا لأن اندماج أنماط الصراع، التي كان يُنظر إليها سابقًا على أنها غير متصلة، هي جوهر التهديدات المختلطة الآن، فمن المنطقي أن تأتي التهديدات المختلطة والحرب المختلطة بأشكال عديدة، وسيستمر هذا التحدي في التطور.

ويؤكد هوفمان على ضرورة استبدال المصطلحات الأمنية القديمة التي أثبتت عدم كفايتها في توصيف الظاهرة مثل "العمليات العسكرية بخلاف الحرب" "Military Operations Other Than War" و"الصراع منخفض الكثافة" Low Intensity Conflict بالمصطلحات الجديدة المعبرة عن ظاهرة الصراع الدولي الجديد[١٣]، وهذا ما عبر عنه Dima Adamsky بمفهومه "**الجيل الجديد من الحرب**" الذي يعبر عن استخدام القوة الصلبة والقوة الناعمة عبر مجالات متنوعة بواسطة التطبيق الماهر للأدوات العسكرية والدبلوماسية والاقتصادية التي تم التنسيق بينها[١٤].

وتؤدي التهديدات الهجين إلى ظهور نوعين من الأفعال الهجين؛ هي **الصراعات الهجين**، والتي ينتج عنها صراعات غير متكافئة asymmetrical

(ISSN: 2536 - 9555)

conflict تنعكس نتائجها على ثلاثة مستويات تشمل ساحة الحرب التقليدية، والرأي العام، والمجتمع الدولي، وتتميز هذه الصراعات بعنصر المفاجأة والحركة الغير مألوفة، والأساليب والتكتيكات العملية الجديدة، وغموض وصعوبة تحديد ماهية العدو، **والحروب الهجين** التي تتجاوز النماذج التقليدية للحروب والتي أشارت اليها الأدبيات في ستة أنواع تشمل حروب ضد الاستعمار، وحروب التحرر الوطني، وحروب ضد الأنظمة العنصرية، وحروب ما بعد الاستعمار، والحروب الأهلية، بالاضافة إلى حروب تفكك الدول الفيدرالية(١٥).

وقدم Andrew Radin ثلاثة سيناريوهات للتهديدات الهجين نابعة من تحليله للحرب الروسية الهجين في منطقة البلطيق تبلورت في(١٦):

أ. **التخريب اللاعنفي** Nonviolent Subversion: الذي يسعى لاستخدام الدعايا والهجمات الالكترونية والتحرك الخفي والوسائل الغير عنيفة من أجل اضعاف نفوذ وحكومات الدول أو التأثير عليها، وكوسيلة للتحكم في قرارات الطرف الآخر واكتساب النفوذ الداخلي واثارة انعدام الاستقرار أو مساعدة الفصائل الموالية للوصول للحكم دون الظهور كطرف مباشر له أي نشاط، ودون الدخول في صراع عسكري.

ب. **التحرك العنيف الخفي** Covert Violent Action: الذي يستخدم فيه القوة المسلحة بطريقة تتعذر نسبتها للدولة التي استخدمتها أو تكون قابلة للانكار، وذلك من خلال ثلاث أنواع من العمليات؛ **الأولى،** عمليات للسيطرة على الدولة المستهدفة من خلال قوات مخفية الهوية يصعب نسب أعمالها إلى دولة معينة، مما يقلل الاستجابة السريعة ورد الفعل لتلك الأفعال، **والثانية،** عمليات تقديم الدعم للحركات الانفصالية من خلال السلاح والمشورة وعدد من القوات، **والثالثة،** عمليات تحريض الحملات الارهابية ضد حكومات الدول المستهدفة.

ت. **العدوان التقليدي المدعوم والمشرع عبر نطاق من الدعايا، أو التحرك الخفي، وغيرها من أشكال الحرب غير النظامية** Conventional Aggression Supported by Political Subversion: يعتمد هذا النوع من الهجوم الهجين على هجوم تقليدي من القوات البرية والبحرية والجوية تبرره وتضفي عليه الشرعية نشاطات خفية يتم انكارها.

بناء على ما سبق يمكن أن نستنتج خصائص لطبيعة التهديدات الهجين تتبلور في:

- تتميز التهديدات الهجينة بعنصر المفاجأة والمرونة والتكتيكات غير التقليدية وصعوبة تحديد طرف الهجوم.
- تؤثر التهديدات الهجينة على الرأي العام الداخلي، وعمل المؤسسات الرسمية، والمجتمع الدولي.
- تستخدم التهديدات الهجينة وسائل غير تقليدية وعلى رأسها الوسائل التكنولوجية لاحداث أثر على الطرف الأخر يتراوح ما بين التهديد، والتخريب، والهجوم العنيف واحداث أضرار جسيمة.
- تزيد فعالية التهديدات بتداخل الأشكال الهجينة مع الأشكال التقليدية.

المحور الثاني
الفضاء السيبراني كمصدر تهديد في العلاقات الدولية

في هذا المحور سيتم تناول مفهوم السيبرانية وتأثيرها كتهديد في تفاعلات ومفاهيم العلاقات الدولية.

١. مفهوم السيبرانية.

أصبح هناك تقاطع بين السيبرانية والذكاء الاصطناعي، وقد مثل مفهوم Norbert Wiener لمصطلح cybernetics أساسا لتعريف الفضاء السيبراني حيث ذكر أن cybernetics هو "التحكم والتواصل في الحيوان والآله[١٧]" بمعنى أن البشر يمكنهم التفاعل مع الآلات وأن النظام الناتج يمكن أن يوفر بيئة بديلة للتفاعل.

وفي أوائل الثمانينيات، اتخذ مؤلف الخيال العلمي ويليام جيبسون الخطوة التالية من خلال صياغة كلمة الفضاء الالكتروني في أحد كتبه. على الرغم من أن هذا حدث في بيئة خيالية، فقد أصبحت الكلمة مستخدمة على نطاق واسع في الأوساط المهنية والأكاديمية. ووصف في كتابه الفضاء الالكتروني بأنه "هلوسة

(ISSN: 2536 - 9555)

توافقية يتعرض لها يوميًا بلايين من المشغلين الشرعيين legitimate operators، في كل دولة، من خلال تعليم الأطفال المفاهيم الرياضية وتمثيل رسومي للبيانات المستخرجة من بنوك كل كمبيوتر في النظام البشري". ويركز هذا التعريف على التصور البشري للبيئة الجديدة، ويوضح إمكانية تطوير تجربة فضاء الكترونية(١٨).

ومع تعدد التعريفات أكد Daniel Kuehl على أن الفضاء السيبراني هو أكثر من مجرد أجهزة كمبيوتر ومعلومات رقمية، وهناك أربعة جوانب للفضاء السيبراني يجب أن يعكسها التعريف هي:

- مساحة تشغيلية An operational space: يستخدم الأشخاص والمؤسسات الفضاء الالكتروني للعمل وإحداث التأثيرات، إما في الفضاء الالكتروني فقط أو عبر المجالات الأخرى.
- مجال طبيعي A natural domain: الفضاء الالكتروني هو مجال طبيعي، يتكون من نشاط كهرومغناطيسي ويتم إدخاله باستخدام التكنولوجيا الالكترونية.
- يستند إلى المعلومات Information based: يدخل الأشخاص إلى الفضاء الالكتروني لإنشاء المعلومات وتخزينها وتعديلها وتبادلها واستغلالها.
- مجموعة شبكات مترابطة Interconnected networks: وجود اتصالات تسمح للنشاط الكهرومغناطيسي بنقل المعلومات.

ويقدم Daniel Kuehl تعريفه الخاص للفضاء الالكتروني ليعكس هذه الجوانب الأربعة حيث عرفه بأنه "مجال عالمي داخل بيئة المعلومات يتم تأطير طابعه المميز من خلال استخدام الالكترونيات والطيف الكهرومغناطيسي لإنشاء المعلومات وتخزينها وتعديلها وتبادلها واستغلالها عبر شبكات مترابطة وباستخدام تقنيات المعلومات والاتصالات"(١٩)، وأضاف كل من Valeriano, and Maness بأنه مجال افتراضي من صنع الانسان يعتمد على نظم الكمبيوتر وشبكات الانترنت وكم هائل من البيانات والمعلومات والأجهزة، كما يعرف بأنه الذراع الرابع للجيوش الحديثة(٢٠).

وقد كان هذا التقدم التكنولوجي آثارا مهمة على التهديدات الأمنية، فظهرت الأسلحة السيبرانية واستخدمت كأداة للاكراه، وأصبحت الهجمات السيبرانية تحدث على مستويين، الأول ""syntactic attacks"" عبر البرامج الضارة من خلال قيام الفيروسات بمهاجمة المستخدمين، والثاني، "semantic attacks" التي تهاجم البنى التحتية أو مرافق تكنولوجيا المعلومات عن طريق تعديل البيانات بشكل غير ملحوظ، وأضحت الحوادث الالكترونية التي تُفهم على أنها اضطرابات في العمليات الروتينية للتقنيات الرقمية، تحتل مكانة بارزة في سياسة الأمن الوطنية والدولية، حيث تحاول الجهات الفاعلة الحكومية إيجاد إجابات مناسبة لمواجهة التهديد الجديد. كما اعتبر الفضاء الاليكتروني فرصة لتغير حسابات توزيع القوة، وحسابات نقاط الضعف والقوة لدى الدول والمنظمات، وزادت الدراسات حول دور التكنولوجيا الرقمية في مجال العلاقات الدولية، ونشأ المفهوم متزامنا مع مفهوم الحرب الشبكية والحرب الاليكترونية ل Arquilla and Ronfeldt عام ١٩٩٣[٢١]، وأصبح الصراع السيبراني والحرب السيبرانية مهيمنين على القضايا ذات الأهمية في العلاقات الدولية. وطرحت فرضيات عديدة بشأن التطور التكنولوجي وتأثيره على المفهوم التقليدي للأمن والتهديدات الأمنية، فذكر "دايفيد هيلد Held" وآخرون في كتاب Globalization Transformation سبع فرضيات أساسية مرتبطة بتطور مفهوم التهديدات والأمن في عصر العولمة، ثلاث منها مرتبط بالتطور التكنولوجي تتبلو في[٢٢]:

- أن العالم يمارس ثورة جديدة في التكنولوجيا العسكرية MTR، فتقنيات المعلومات، تحول القدرات العسكرية الموجودة، وإدارة الحروب، والقدرة على إظهار القوة العسكرية من مسافات بعيدة بدقة عظيمة.
- أن أنظمة الاتصالات الآنية تجعل إدارة الحروب أسهل، لأن القادة يستطيعون الإشراف والتدخل بالعمليات العسكرية الميدانية إلى درجة لم تكن ممكنة من قبل.

(ISSN: 2536 - 9555)

- أن العولمة المتزايدة في قطاعات الصناعات المدنية التي تعمل في الإنتاج الدفاعي للاكترونيات أو البصريات، تجعل الحصول على الأسلحة واستخدامها خاضعا لقرارات اعمال سلطات أخرى من غير الدولة.

٢. تطور طبيعة التهديدات السيبرانية وتأثيرها في العلاقات الدولية.

ظهرت أهمية الفضاء السيبراني السياسية من خلال مفاهيم عديدة مرتبطة باستخدامه ومنها مفهوم **القوة السيبرية cyber power** التي ترتبط بالقضايا السياسة من خلال مفهوم "**النفوذ**"، فالسياسة تدور حول توزيع النفوذ، والقوة السيبرية هي سلالة أخرى من محاولات السيطرة على النفوذ والقوة في السياقات الدولية والمحلية، وبالتالي تعتبر القوة السيبرية هي القدرة على تطبيق أشكال نموذجية للسيطرة والهيمنة في الفضاء الالكتروني، ومن هنا لعب الفضاء السيبراني دورا أساسيا في تعظيم القوة، أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية، فمثل التفوق في ذلك المجال عنصرا حيويا في تنفيذ عمليات ذات فاعلية سواء على الأرض أو في البحر أو الجو أو حتى في الفضاء، ومع اعتماد القدرة القتالية في الفضاء الالكتروني على نظم التحكم والسيطرة التكنولوجية[٢٣]، تغير مفهوم القوة الوطنية للدولة، وأصبحت تعبر عن "كل الوسائل، والطاقات، والإمكانيات سواء المادية أو غير المادية، والمنظورة وغير المنظورة التي بحوزة الدولة، ويستخدمها صانع القرار في أفعال تؤثر في سلوك الوحدات السياسية الأخرى وتحقق مصالح الدولة"، وترتكز عناصر القوة السيبرية على خلق التناغم بين القدرات التكنولوجية، والسكانية، والاقتصادية، والصناعية، والقوة العسكرية، وإرادة الدولة، وغيرها لايجاد نظام متماسك يعظم القوة المتحصلة ويسهم في دعم إمكانات الدول على ممارسة الإكراه، أو الإقناع، أو ممارسة التأثير السياسي في أعمال الدول الأخرى بغرض الوصول للأهداف الوطنية، من خلال قدرات التحكم، والسيطرة على الفضاء الإلكتروني[٢٤].

وبالتالي أعطت القوة السيبرانية دفعا رئيسيا في اتجاهين، **الأول:** تدعيم القوة الناعمة للدول، حيث بات الفضاء الالكتروني مسرحا لشن هجمات تخريبية ترتبط

بنشر المعلومات المضللة، والحرب النفسية، والتأثير في توجهات الرأي العام، والنشاط السري والاستخباراتي. أما **الاتجاه الآخر**، فيتعلق بتبني الدول لزيادة الإنفاق في سياسات الدفاع الالكتروني، وحماية شبكاتها الوطنية من خطر التهديدات، وبناء مؤسسات وطنية للحماية الالكترونية.

وقد أثرت الطبيعة الجديدة للتهديدات السيبرانية وما لحق بها من تطورات على حقل العلاقات الدولية سواء على المستوى المفاهيمي أو مستوى التفاعلات الدولية .

أولا: على المستوى المفاهيمي: (القوة- الأمن)

أثرت التطورات في شكل التهديدات في عصر الثورة التكنولوجية على مفهومي القوة والأمن في العلاقات الدولية من خلال:

أ. **تغير مصادر القوة وتعدد فواعلها**، لقد أدت ظاهرة الفضاء الالكترونى الى تحول جزء من العالم من الطابع المادى إلى عالم رقمى الكترونى، وأصبح الفضاء الالكترونى مجال جديد للتفاعلات الدولية سواء أكانت تفاعلات صراعية أو تعاونية، وأثر ذلك على تغير طبيعة القوة وبروز تهديدات الفضاء الالكترونى، وامكانية احداث ضرر دون تدخل عسكري مباشر، وأثر ذلك بدوره على استراتيجيات الأمن القومى للدول، والسعى إلى الاستحواذ على مصادر القوة داخل الفضاء الالكترونى لمنع تعرض بنيتها التحتية والحيوية للخطر[٢٥]، ومن ثم دخل المجال الالكترونى ضمن المحددات الجديدة للقوة وأبعادها الجديدة من حيث طبيعتها وأنماط استخدامها وطبيعة الفاعلين فيها، أدى ذلك إلى تعزيز القوة وانتشارها. فمن جهة، عزز الفضاء الالكتروني ما يسمي بـ **"القوة المؤسسية"** في السياسة الدولية[٢٦]، وهي تعني أن يكون لها دور في قوة الفاعلين، وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والإسهام في تشكيل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة،

(ISSN: 2536 - 9555)

والتي تؤثر في تشكيل السياسة العالمية. ومن جهة أخرى، عمل الفضاء الالكتروني على إعادة تشكيل قدرة الأطراف المؤثرة وتنوعها، حيث برزت عملية انتشار القوة بين أطراف متعددة، سواء أكانت دولا، أم من غير الدول، ومن ثم اعادة توزيع القوة بين الدولة القومية والفاعلين من غير الدول.

ب. **التأثير على وسائل القوة**، تطورت وسائل القوة وبرز مفهوم **القوة الاليكترونية** كنوع من أنواع القوة التي أشارت إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل"[٢٧]، أدى ذلك إلى التأثير على الوسائل التقليدية للقوة؛ فأثرت القوة الالكترونية على **تعظيم دور "الأدوات الرمزية"**، حيث لعبت دور مهم فى التأثير على أفكار الأطراف الآخرى سواء النخب أو الجماهير، كما أثرت على القوة العسكرية، وظهرت الأسلحة السيبرانية واستخدام الفيروسات الالكترونية فى شن الهجمات أو سرقة المعلومات، واستخدامها كقوة ناعمة فى الحرب النفسية والتأثير على الرأى العام، أثرت أيضا على القوة الاقتصادية التقليدية، فنمى دور الاقتصاد الرقمى، ونمت التجارة الالكترونية، وأصبح على كل دولة ترغب فى بناء اقتصاد قوى أن تهتم بالاستثمار فى التكنولوجيا، ورفع مستوى التعليم التقنى داخل الدولة، بالاضافة إلى تطور الأدوات الاستخباراتية من حيث سهولة جمع المعلومات، والتصنت والتجسس وتسهيل النشاطات السرية فى العلاقات الدولية مثل عملية الاغتيالات.

ج. **بروز مفاهيم جديدة في العلاقات الدولية:** شهد حقل العلاقات الدولية أشكال جديدة من التفاعلات أدت إلى بروز مجموعة من المفاهيم في الدراسات الأكاديمية الخاصة بحقل العلاقات الدولية ومنها؛ "**سباق التسلح السيبراني**" cyber arms race، الذي اشتعل منذ عام ٢٠٠١ بين الولايات المتحدة وايران، وكذلك بين كوريا الشمالية وكوريا الجنوبية[٢٨]، ومفهوم "**الهيمنة على**

الفضاء السيبراني" خاصة بعد مقترح القوة الفضائية الأمريكية الذي حرص الرئيس ترامب بالبدء فيه كتمهيد لانشاء فرع عسكري جديد في الفضاء وذلك كخطوة علنية نحو "**عسكرة الفضاء**" من أجل الحفاظ على الهيمنة العالمية، وتحقيق هيمنة استراتيجية على القوى المنافسة مثل الصين وروسيا، وذلك من خلال إنشاء وكالة تنمية فضائية، وقوة عمليات فضائية، بالاضافة إلى إنشاء قيادة فضائية للتصدي لحروب الفضاء[٢٩]، وقد أدى ذلك إلى تطور مجال سياسات الدفاع والأمن الالكتروني، متمثله في تصاعد وتيرة سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.

د. **صعود الأمن السيبراني ومفهوم الردع الجديد**[٣٠]: يعتبر الأمن السيبراني مستوى سادس من مستويات الأمن المتعددة سواء العسكري، السياسي، الاقتصادي، البيئي، المجتمعي، وقد شكل الأمن السيبراني نوعا من الأمن الجماعي العالمي، خاصة مع وجود مخاطر تهدد الفاعلين في مجتمعات المعلومات العالمي مما فرض إعادة تفكير في الأمن القومي للدولة خاصة أن الأخير صار جزءا من الأمن العالمي، هذا النوع من الأمن ارتبط بترسيخ نوع من أنواع "الردع السيبراني" **cyber deterrence**، فبالقياس بالردع النووي الذي أحال دون حدوث مواجهة مباشرة بين الولايات المتحدة الأمريكية والاتحاد السوفيتي وقت الحرب الباردة، جادل Hanna Samir Kassab بأن الهجوم السيبراني لتكلفته المرتفعة يؤسس لما أطلق عليه "الردع السيبراني" مما يقلل احتمالية الصدام بين الفواعل المختلفة ويعمل على تحقيق ما يطلق عليه "الأمن السيبراني في العلاقات الدولية".

هـ. **الأمن الدولي متعدد المستويات**[٣١]: أدى بروز الأمن السيبراني إلى وجود فواعل عديدة من غير الدول مثل شركات الأمن الخاصة في مجال التكنولوجيا، وشبكات الجريمة الالكترونية وشبكات القرصنة الاليكترونية والجماعات الارهابية وغيرها من الفواعل التي فرضت تحديات عديدة في

(ISSN: 2536 - 9555)

الحفاظ على الأمن السيبراني العالمي وأنتجت معها مستويات متعددة من الأمن وجب التنسيق فيما بينها لضمان تحقيق الأمن العالمي.

ثانيا: على المستوى التفاعلات الدولية (الصراع- الحرب):

أ. **تغير نمط الصراع في العلاقات الدولية:** رصد التقرير الصادر عن وزارة الدفاع البريطانية في عام ٢٠١٠ بعنوان "الطابع المستقبلي للصراع" الاستخدام المتزايد للفضاء السيبراني كمنصة لشن الصراعات والنزاعات بشكل مباشر وغير مباشر بين الفواعل المختلفة[٣٢]، وصعد **"الصراع السيبراني" cyber conflict** كحالة من التعارض في المصالح والقيم بين الفاعلين، سواء أكانوا دولا أم غير دول في الفضاء الالكتروني، فأصبحت أجهزة الاستخبارات الدولية تختبر شبكات الدول الأخرى بصورة دورية بحثا عن ثغرات وتزداد أساليبها تطورا باستمرار، وشهدت العديد من الدول هجمات سيبرانية كان من بينها الولايات المتحدة والهند وألمانيا وفرنسا وبريطانيا عام ٢٠٠٧ بالإضافة إلى الهجوم على استونيا في نفس العام، وفي الحرب الجورجية الروسية في ٢٠٠٨ تطورت الهجمات الالكترونية من مجرد عمليات بحث بدافع الفضول إلى عمليات جيدة التمويل والتنظيم تشمل التجسس السياسي والعسكري والاقتصادي والتقني، وتم الكشف عن شبكة تجسس الكترونية تعمل في الصين تمكنت من اختراق ١٢٩٥ جهاز كمبيوتر في ١٠٣ دوله وتعد الحادثة الاكبر في العالم من حيث عدد الدول التي تم اختراق شبكاتها واجهزتها منها وزارات خارجية كل من ايران وبنجلاديش ولاتفيا واندونيسيا والفلبين وبروناي وتايلاند وبوتان. وتم اكتشاف اجهزة تنصت على الكمبيوتر في سفارات كل من الهند وكوريا الجنوبية واندونيسيا وقبرص ومالطا وتايوان والبرتغال والمانيا وباكستان، وهناك نحو ١٢٠ دولة تقوم بتطوير طرق لاستخدام الإنترنت كسلاح لاستهداف أسواق المال ونظم الكمبيوتر الخاصة بالخدمات الحكومية[٣٣]. وقد تميز **الصراع السيبراني** بصعوبة تحديد أطرافه، والزيادة المطردة في أعداده، والآثار الخطيرة التي يحدثها في أمن الدول، كما أن

طبيعته الصراعية ممتدة، مما نتج عنه إعادة التفكير في حركية وديناميكية الصراع وظهور ما يعرف ب "**عصر القوة النسبية**" التي أشارت إلى أن "القوة العسكرية" قد لا تكفي وحدها لتأمين البنية التحتية للدول، الأمر الذي يخلف آثارا استراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولي، وقد شملت الصراعات السيبرانية على[٣٤]:

- **الصراع السيبراني السياسي:** وغايته تحقيق أهداف سياسية من خلال صراع سيبراني عسكري هجومي يعمل على افساد النظم المعلوماتية والشبكات البنية التحتية من خلال استخدام الأسلحة الالكترونية من قبل فاعلين داخل المجتمع المعلوماتي.
- **الصراع السيبراني الناعم:** ويعمل على التأثير في الأفكار والرأي العام من خلال الحرب النفسية والاعلامية وتسريب المعلومات التي لها بعد دولي يؤثر على العلاقات الدولية.
- **صراع سيبراني تكنولوجي:** يركز على سباق التقدم التكنولوجي والحصول على المعلومات والتحكم بها واستخدامها لاختراق الأمن القومي للدول والتأثير على اقتصادها.
- **الصراع السيبراني الاستخباراتي:** حيث تعمل الأجهزة الأمنية للدول لدعم قدراتها الاستخباراتية وشبكة عملائها المختلفة من خلال استخدام الوسائل الالكترونية في التجسس وجمع المعلومات لصعوبة الرقابة على التفاعلات الالكترونية وسهولة الاتصال ولتحقيق أهداف سياسية وعسكرية.

ب. **تطور شكل الحروب:** ظهرت أنماط جديدة من الحروب عرفت باسم **الحرب السيبرانية cyber war** التي تعددت تعريفاتها ما بين تعريفات ضيقة تتناول الغرض من الحرب مثل تعريف Lionel D. Alford (٢٠٠١)[٣٥] الذي عرفها بأنها "امكانية التحكم في برامج السوفت وير الخاصة بالمعارضين لفرض ارادة الدولة الوطنية"، وحدد هنا الهدف والفاعل، أو تعريفات واسعة النطاق مثل تعريف كل من Parks and Duggan[٣٦] بأنها "عبارة عن مزيج

(ISSN: 2536 - 9555)

من هجوم شبكات الكمبيوتر والدفاع والعمليات الفنية الخاصة"، ويعتبر هذا التعريف تعريف واسع جدًا للحرب السيبرانية يتجنب مسألة من يشارك ولماذا، كما قدم Robinson.[٣٧] تعريف للحرب السيبرانية معتمدا على الفاعل Actor، ونية الفعل Intent؛ بحيث يفرق بين الدولة كفاعل أو جماعة ارهابية، أو فرد، كما يفرق بين نيه الفعل بسؤال ما هو الغرض من الضرر، هل هو تحقيق أهداف عسكرية، أو كسب شخصي، أو لأغراض التجسس، أو التأثير على سياسات الدولة، وخلص إلى أن الحرب يطلق عليها حرب سيبرانية عندما تكون هي النوع الوحيد المستخدم لاحداث ضرر عسكري، وفي هذه الحالة يطلق عليها "cyber war"، أما اذا كانت أداة بجانب الحرب الحركية kinetic attack، فتعتبر "cyber warfare"، ولا تقتصر الحرب السيبرانية على الدول كفاعل أساسي، بل شملت الفواعل الأخرى ومنها الجماعات الارهابية التي أطلق على عملياتها السيبرانية مصطلح **الارهاب الاليكتروني cyber terrorism** ليشير المصطلح إلى "الهجمات الالكترونية التي تهدف إلى تخويف أو إكراه السكان المدنيين، أو التأثير على سياسة الحكومة عن طريق الترهيب أو الإكراه، ليصبح الارهاب السيبراني مرحلة من مراحل الحروب السيبرانية ضد الدول والجماعات، وقد أسهم عاملان في زيادة هذا النوع من الحرب، **الأول** هو **تغير المنظور المعتاد للحرب**، من حيث الهدف والطريقة؛ فانتقلت الحروب من هدف تدمير الخصم، إما باحتلال أرضه، أو الاستيلاء على موارده، إلى محاولة التحكم في إرادة وخيارات المجتمعات والتأثير على الرأي العام، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة، أو بالرأي العام في الدولة التي تشن الحرب، أو بالرأي العام على الصعيدين الإقليمي والدولي، وبالتالي ركزت الحرب على العامل النفسي والدعائي، لاسيما مع تنامي التغطية الإخبارية، والسمعية، والبصرية المباشرة للأحداث لحظة وقوعها عبر مواقع الإنترنت والفضائيات، وضعف سيطرة أنظمة الحكم على توجهات مواطنيها، **العامل الثاني** هو **بروز**

الصراعات ذات الأبعاد المحلية– الدولية، وذلك من خلال توفير بيئة مناسبة لدمج الفئات المهمشة في السياسة الدولية نتيجة توفير بيئة مناسبة لهم نتيجة اشتعال الصراعات الداخلية في مرحلة ما بعد الحرب الباردة، وكذلك لطبيعة السياق الدولي للفضاء الالكتروني الذي عمل على خلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض، إما على أساس قيم حقوقية، أو انتماءات عرقية أو دينية، وقد تنوعت أنماط الحروب السيبرانية فتراوحت بين ما يلي:

- **الحرب السيبرانية الباردة منخفضة الشدة**[٣٨]: في هذا النوع من الحرب يتم استخدام الفضاء الالكتروني كساحة للصراع منخفض الشدة الذي قد يكون ذا طبيعة ممتدة له طابع غير سلمي بخلاف أنه عميق الجذور ومتداخل، وله نواح متعددة ثقافية، أو اقتصادية، أو اجتماعية. وعادة ما يتم اللجوء إلى القوة الناعمة للحروب السيبرانية في مثل صراعات كهذه، وإن كانت لا تتطور بالضرورة إلى استخدام القوة المسلحة بشكلها التقليدي، أو شن حرب الكترونية واسعة النطاق، وتجلى هذا النمط في حالات الحروب في الصراعات السياسية، ذات البعد الاجتماعي– الديني الممتد، مثل الصراع العربي– الإسرائيلي، أو الصراع الهندي– الباكستاني.
- **نمط "الحرب" السيبرانية متوسطة الشدة**[٣٩]: حيث يتحول الصراع عبر الفضاء الالكتروني إلى ساحة موازية لحرب تقليدية دائرة على الأرض. ويكون ذلك تعبيرا عن حدة الصراع القائم بين الأطراف، كما قد يمهد لعمل عسكري. هنا تدور حروب الفضاء الالكتروني عن طريق اختراق المواقع الالكترونية، وتخريبها، وشن حرب نفسية ضد الخصوم، ويستمد ذلك النوع من الحروب السيبرانية شدته من قوة أطرافه، وارتباطها بعمل عسكري تقليدي، مثل هجمات حلف الناتو في عام ١٩٩٩ على يوغوسلافيا.
- **نمط الحرب السيبرانية الساخنة مرتفعة الشدة**[٤٠]: حيث يعبر ذلك النمط عن نشوء حروب في الفضاء الالكتروني منفردة، وغير متوازية مع الأعمال

(ISSN: 2536 - 9555)

العسكرية التقليدية، وينطوي هذا النمط من الحروب على سيطرة البعد التكنولوجي على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الالكترونية فقط ضد منشآت العدو، وكذا اللجوء إلى الروبوتات الآلية في الحروب والطائرات دون طيار، وإدارتها عن بعد، بخلاف تطوير القدرات في مجال الدفاع والهجوم الالكتروني، والاستحواذ على القوة الالكترونية.

- **نمط الحرب "بالوكالة السيبرانية[٤١]" Proxy War in Cyberspace**، ويشير إلى شن الحروب بشكل غير مباشر بتوظيف فواعل أخرى لتحقيق أهداف الدول مثل المرتزقة، والقراصنة والميليشيات السيبرانية، وفي المقابل قد يستغل فاعل من غير الدول بعض الدول الهشة للعمل من خلالها، أو قد يوظف فاعلا آخر على شاكلته كاستعانة القراصنة ببعضهم البعض لتحقيق مختلف الأهداف، وهو ما تجلى في الحرب الروسية الجورجية عام ٢٠٠٨.

المحور الثالث
الذكاء الاصطناعي كمصدر تهديد في العلاقات الدولية

يتناول هذا المحور مفهوم الذكاء الاصطناعي وتوضيح تأثيراته الحالية والمحتملة كتهديد على الساحة الدولية.

١. مفهوم الذكاء الاصطناعي:

على مدار الخمسة عشر عامًا الماضية، أدى مزيج من ثلاثة عوامل شملت الزيادة السريعة في قوة الحوسبة، والزيادة الهائلة في البيانات، وتحسين الخوارزميات، إلى ظهور موجة جديدة من التقدم في أبحاث الذكاء الاصطناعي Artificial Intelligence (AI)، لا سيما في المجال الفرعي للتعلم الآلي Machine Learning (ML) ومجموعته الفرعية من التعلم العميق. منذ ذلك الحين، شقت تطبيقات الذكاء الاصطناعي المتنوعة التي تم تطويرها في مختبرات الشركات والجامعات طريقها إلى الاستخدام العملي اليومي[٤٢]، وقد بدأ الحديث عن الذكاء الاصطناعي بالظهور في مرحلة مبكرة كمشروع لدارتموث البحثي الصيفي لعام ١٩٥٦ حول الذكاء الاصطناعي من خلال اقتراح قدم إليه في ٣١

أغسطس ١٩٥٥، من قبل جون مكارثي، الأب المؤسس للذكاء الاصطناعي، ومارفن مينسكي وناثانيال روتشستر وكلود شانون، وكانت الفرضية الأساسية للدراسة هي أن كل جانب من جوانب التعلم أو سمة أخرى من سمات الذكاء يمكن من حيث المبدأ وصفها بدقة بحيث يمكن صنع آلة لمحاكاتها من خلال محاولة جعل الآلات تستخدم اللغة، وتحل أنواع المشاكل المخصصة للبشر، وتحسن نفسها تلقائيا(٤٣).

كما عرف Kurzweil وآخرون في مقاله لهم عام ١٩٩٠ الذكاء الاصطناعي بأنه "الآلات التي يمكنها القيام بمهام تتطلب ذكاء عندما يؤديها البشر"(٤٤)، ويعمل الذكاء الاصطناعي بشكل أساسي من خلال التعلم الآلي، والذي يشير إلى قدرة النظام على تحسين الأداء دون الحاجة إلى بشر لشرح كيفية إنجاز المهمة المحددة، وقد تم تحقيق معظم النجاحات في السنوات الأخيرة بمساعدة ما يسمى التعلم الخاضع للإشراف supervised learning، حيث يتم إعطاء الآلة العديد من الأمثلة للإجابة الصحيحة لمشكلة ما(٤٥).

وقد حددت الدراسات أربعة دوافع رئيسية وراء التقدم السريع في تكنولوجيا الذكاء الاصطناعي تبلورت في(٤٦):

أ. عقود من النمو المتسارع في أداء الحوسبة.

ب. زيادة توافر مجموعات البيانات الكبيرة التي يمكن على أساسها تدريب أنظمة التعلم الآلي.

ج. التقدم في تنفيذ تقنيات التعلم الآلي.

د. الاستثمار التجاري الكبير والمتزايد بسرعة.

وهناك أنواع من الذكاء الاصطناعي التي يقصد بها مدى قدرة الآلة على محاكاة وظائف البشر والعقل الانساني بدقة فائقة؛ وبالتالي يتم تصنيف أنواع الذكاء الاصطناعي وفقا لطريقتين:

الطريقة الأولى(٤٧): تصنف الذكاء الاصطناعي ما بين ثلاثة فئات، الفئة الأولى هي الذكاء الاصطناعي الضيق، والفئة الثانية هي الذكاء الاصطناعي العام، أما الفئة الثالثة فهي الذكاء الاصطناعي الفائق، ويختلفوا من حيث عدد

(ISSN: 2536 - 9555)

المهام التي يمكنهم القيام بها والقدرات الخاصة بهم، فيمكن أن يؤدي الذكاء الاصطناعي الضيق مهمة واحدة أو عدة مهام محددة. مثل اكتشاف المرضى للسرطان أو الحكم على الجدارة الائتمانية للعملاء، وقد حققت هذه التطبيقات المحدودة القدرة للذكاء الاصطناعي تقدمًا سريعًا في السنوات الماضية، وأثبت بعضها أنها ذات قيمة عالية، إلا أنها لا تتخطى المهام المصممة لها، أما الذكاء الاصطناعي العام، الذي يهدف إلى أداء معظم الأنشطة التي يمكن للبشر القيام بها بالاضافة إلى إمكانية بناء قدرات متنوعة، لا يزال هناك العديد من الأسئلة المفتوحة لبناء القدرات اللازمة لتحقيقه، أما الذكاء الاصطناعي الفائق فيمثل تطويره ذروة الأبحاث التي تسعى لأن يكون أكثر أشكال الذكاء قدرة على الأرض وسيتميز بالقدرة الفائقة وعدد المهام اللامحدودة بحيث يقوم بالمهام بشكل أفضل من الانسان.

الطريقة الثانية[٤٨]: تعتمد على تصنيف الآلات وفقا لتشابهها مع العقل البشري، وتشمل الآلات التفاعلية التي تتمتع بقدرة محدودة للغاية بحيث تستجيب لأنواع مختلفة من المحفزات وتحاكي العقل البشري ولكنها لا توظف الذاكرة ولا تستفيد من خبراتها السابقة، ومن أمثلتها أجهزة Deep Blue التي طورتها شركة أي بي أم وفازت على بطل الشطرنج ١٩٩٧، هناك الآلات محدودة الذاكرة والتي يمكن أن توظف البيانات السابقة في اتخاذ القرارات الحالية ومنها السيارات ذاتية القيادة، أما النوع الثالث من الآلات فهو الذي يعتمد على "نظرية العقل" التي تعمل على فهم الكيانات التي تتفاعل معها بشكل أفضل، أما الفئة الأخيرة والتي مازالت ضمن حدود الإفتراضات، فهي الآلات المعتمدة على "الوعي الذاتي" التي تطور نفسها ذاتيا دون أي تدخل خارجي.

وبناء على ما سبق يمكن للدراسة أن تعرف الذكاء الاصطناعي بأنه "قدرة الآلات والحواسيب الرقمية على محاكاة مهام البشر، كالقدرة على التفكير أو الإدراك البصري والتعرف على الكلام وصنع القرار أو التعلم من التجارب السابقة أو غيرها من العمليات التي تتطلب عمليت ذهنية، وتتفاوت هذه القدرة وعدد المهام حسب كل نوع من أنواع الذكاء الاصطناعي، إلا أنه في المجمل يمكن للذكاء الاصطناعي الاستنتاج، واكتساب المعرفة الجديدة وادراك الأشياء

ومعالجتها والتعلم من خلال الاحتفاظ في الذاكرة بالتجارب السابقة، ولها قدرات تحليلية وتنبؤية وتشغيلية متطورة".

٢. تأثير تقنية الذكاء الاصطناعي في العلاقات الدولية:

في السنوات العديدة الماضية أصبحت لتطبيقات الذكاء الاصطناعي أدوارا متعددة، كما أصبحت فاعلة في العلاقات الدولية خاصة في المجالات المتعلقة بالأمن، بما في ذلك الاستخبارات والدفاع والسياسة العسكرية وسياسة الأمن الخارجي (الحد من الأسلحة) والأمن الداخلي (أمن الدولة والشرطة وحماية الحدود وإدارة الكوارث وحماية البنى التحتية الحيوية). ومع ذلك فإن فهم كيفية تفاعل الذكاء الاصطناعي مع الأمن القومي والعالمي، الآن وفي المستقبل مازال في حاجة إلى مزيد من الوضوح.

تلعب التقنيات أدوارًا شديدة التناقض في السياسات الأمنية المعاصرة. بالنسبة للبعض، فإن الاختراعات مثل تكنولوجيا النانو أو الروبوتات الآلية أو الأسلحة الذكية أو الهندسة الحيوية هي الأسباب الجذرية للمشاكل المجتمعية الجديدة، وبالنسبة للآخرين، تقدم التقنيات حلولًا فعالة للتهديدات الأمنية المعاصرة. وبينما يستمر الجدل حول ما إذا كانت التكنولوجيا جزءًا من المشكلة أم جزءًا من الحل، يتقارب الرأيان في تقديرهما للأهمية الكلية للتكنولوجيا في تعزيز أو مواجهة المشاكل الأمنية المعاصرة وأنها أساسية لسياسات الأمن الحديثة[٤٩].

على الرغم من أن بعض المنظمات العسكرية قد أبدت بالفعل اهتمامًا بالذكاء الاصطناعي خلال الحرب الباردة، إلا أن ارتباطًا أوسع بين الذكاء الاصطناعي والعلاقات الدولية والسياسة الأمنية ظهر فقط بعد نشر الحكومة الأمريكية لثلاثة تقارير استراتيجية عن الذكاء الاصطناعي في عام ٢٠١٦، خلال ادارة أوباما، وقد شاركت تلك التقارير في استنتاج غير عادي مؤداه أن التطورات في التعلم الآلي، وهي تقنية تسمح للأنظمة بالتعلم والتحسين دون برمجة واضحة، ستكون القوة الدافعة وراء التحولات عبر كل من الاقتصاد والأمن القومي نظرا لأن أنظمة

(ISSN: 2536 - 9555)

الذكاء الاصطناعي أصبحت قادرة بشكل متزايد ليس فقط على انجاز المهام الروتينية مثل قيادة سيارة، بل أيضا على انجاز المهام المعقدة مثل تصميم محرك السيارة(٥٠). ومن هنا سلطت هذه التقارير الضوء على الإمكانات الواسعة النطاق للذكاء الاصطناعي عبر المجالات المختلفة، وبالتالي حفزت العديد من الحكومات على تقييم قدرات الذكاء الاصطناعي الخاصة بها، مما دفع ٢٩ دولة إلى تطوير استراتيجيات وطنية في هذا المجال. في حين أن تأكيدات هذه الاستراتيجيات تختلف، إلا أنها تشترك في الرغبة في خلق أفضل الظروف الممكنة لدولهم للاستفادة من التقدم الذي تم إحرازه مؤخرًا في ذلك المجال. وبشكل عام، من المتوقع أن يقود الطابع الثوري المنسوب للذكاء الاصطناعي وتطبيقه الواسع النمو الاقتصادي، وفي الوقت نفسه، يُفترض أن يكون لها تأثيرًا على مسائل الأمن الوطني والدولي(٥١).

وعلى المدى القصير، من المرجح أن تسمح التطورات في الذكاء الاصطناعي بمزيد من الدعم الآلي المستقل لرجال الحرب، حيث سيوفر التقدم التكنولوجي أعظم المزايا للجيوش الكبيرة وذات التمويل الجيد والمتطورة تقنيًا، تمامًا كما فعلت المركبات الجوية بدون طيار (UAVs) والمركبات الأرضية غير المأهولة (UGVs) في العمليات العسكرية الأمريكية في العراق وأفغانستان. ومع انخفاض الأسعار في المستقبل، ستتبنى الدول ذات الميزانية المحدودة والجيوش الأقل تقدمًا من الناحية التكنولوجية وكذلك الجهات الفاعلة غير الحكومية التكنولوجيا كخيار أساسي لها، وقد تمت ملاحظة هذا النمط اليوم في استخدام تنظيم الدولة الإسلامية الطائرات بدون طيار التي يتم التحكم فيها عن بعد بشكل ملحوظ في عملياته العسكرية. ومن المرجح أن تستخدم الجماعات الارهابية في المستقبل بشكل متزايد المركبات ذاتية القيادة. على الرغم من أن التطورات في مجال الروبوتات والاستقلالية ستزيد من القوة المطلقة لجميع أنواع الجهات الفاعلة، إلا أن توازن القوة النسبي قد يتحول أو لا يتحول بعيدًا عن الدول القومية الرائدة. حيث سيتم التغلب في النهاية على قيود الحجم والوزن والطاقة التي تحد حاليًا من

الاستقلالية المتقدمة، تمامًا كما تقدم الهواتف الذكية اليوم ما كان في السابق أداء الكمبيوتر الفائق(٥٢).

وفي تقرير صدر عن مؤسسة تشاثام هاوس (المعهد الملكي للشئون الدولية) يونيو ٢٠١٨، الذي يحاول فيه قياس آثار الذكاء الاصطناعي والشئون الدولية على المدى القصير والمتوسط، ذكر أن تأثير التكنولوجيا في المجال السياسي تتسم بكثير من التعقيد، وبالرغم من ذلك فانها تلعب دور مهم وفعال في معاونة متخذي القرار على المدى القصير من خلال توفير المعلومات وتحليلها وامكانيات التنبؤ، لكن من الصعب تصور أن تحل تكنولوجيا الذكاء الاصطناعي محل التنفيذيين في صنع القرار في المدى القصير والمتوسط(٥٣).

وبالرغم من أن مرحلة تأثير تقنيات الذكاء الاصطناعي في العلاقات الدولية في مرحلة البلورة إلا أنه يمكن رصد بعض الملامح لهذا التأثير تتبلور في:

أولا: التأثير في صنع السياسة الدولية والقرار الدولي: يلعب الذكاء الاصطناعي دورا في صنع القرار الدولي من خلال آليات التنبؤ المبكر بالمخاطر وبناء نماذج متعددة من القرارات السياسية، وتوفير مستويات أعمق من المعرفة، خاصة أن وفرة المعلومات وامكانية تحليلها يعتبر عنصر من عناصر القوة في عالم العلاقات الدولية، فزيادة التطور التكنولوجي للدولة ينعكس في تطور نفوذها الدولي وزيادة قوتها العسكرية، **ويمكن تصنيف ثلاثة أدوار رئيسية للذكاء الاصطناعي في السياسة الدولية وصنع القرار الدولي تشمل(٥٤):**

أ. **الأدوار التحليلية Analytical roles:** تعمل أنظمة الذكاء الاصطناعي في الأدوار التحليلية، وتمشيط مجموعات البيانات الكبيرة واستخلاص النتائج بناءً على التعرف على الأنماط المتكررة، وهذه هي على وجه التحديد المهام التي تعتبر عمومًا ذات أولوية قصوى للأتمتة، وبالتالي يمكن الاستعانة بها في الاتفاقيات والبروتوكولات الخاصة بالأسلحة وأنواعها، بالاضافة إلى كل ما يتطلب تحليل مجموعة هائلة من البيانات تحتاج إلى متدربين على أعلى مستوى، وبالتالي سيصبح الذكاء الاصطناعي أكثر أهمية في كيفية رؤية صانعي السياسات للعالم وفهمهم له. قدرتها الفعالة على معالجة المعلومات.

(ISSN: 2536 - 9555)

ب. **الأدوار التنبؤية Predictive roles:** قد تكون مجموعة أخرى من الأدوار للذكاء الاصطناعي هي التنبؤ بدلاً من التحليل. بعبارة أخرى، في حين أن التطبيقات التحليلية للذكاء الاصطناعي تهدف إلى تبسيط العمليات الحالية، فقد توفر أنظمة الذكاء الاصطناعي فرصًا لواضعي السياسات لفهم الأحداث المستقبلية المحتملة، أحد الأمثلة في ميدان الشؤون الدولية هو إمكانية صياغة مفاوضات معقدة من خلال استخدام أنظمة الذكاء الاصطناعي للتنبؤ بمواقف الأطراف الأخرى، ومع تكرار العملية تكون نماذج التنبؤ أكثر دقة.

ث. **الأدوار التشغيلية/ التنفيذية Operational roles:** الفئة الأخيرة مختلفة نوعًا ما، فهي تغطي الأنظمة المستقلة بالمعنى التقليدي للروبوتات. من المحتمل أن تكون الآثار المترتبة على هذه التطبيقات منتشرة وغير مباشرة، لكن أهميتها المحتملة تستدعي النظر فيها جنبًا إلى جنب مع الوظائف التحليلية والتنبؤية، فمن المرجح أن يكون للأنظمة اللوجيستية المستقلة آثار كبيرة غير مباشرة على السياسة الدولية. لا يُتوقع أن يتغير الأداء اليومي للنظام الدولي بشكل ملحوظ إذا تم استبدال سائقي الشاحنات أو أطقم السفن أو الطيارين بآلات آلية، ولكن الاستبدال الواسع النطاق للعمالة البشرية الحالية بهذه القدرات من المرجح أن يتسبب في تداعيات اقتصادية واسعة النطاق، بالاضافة إلى اضطرابات سياسية على المدى القصير والمتوسط، وذلك بسبب التشغيل الذاتي للأسلحة المستقلة والجدل العام حول شرعية تطوير واستخدام هذه الأسلحة، بالاضافة إلى أن ذلك التطور قد يتيح تطوير فئات جديدة من الأسلحة تخلق نماذج جديدة تماما للقدرة العسكرية تعتمد على أسلحة اليكترونية مشبعة بالاستقلالية والتعلم الآلي والقدرة على التكيف[٥٥].

ثانيا: التأثير على الجوانب الأمنية والعسكرية: من خلال اشعال سباق التسلح العالمي بين الدول الكبرى خاصة في مجال تطوير أجيال جديدة من الأسلحة التي تعتمد على التقنيات التكنولوجية العالية والانسان الآلي، وتعدد أنواع التطبيقات

العسكرية التي تدخل تحت تصنيف تقنيات الذكاء الاصطناعي والتغيير في سير العمليات المسلحة التي تعتمدها الدول في مواجهة التحديات العسكرية وزيادة اعتمادها ومنها الدرونز الجوية والبرية والبحرية، وأسراب الدرونز الصغيرة الحجم والقادرة على الانتشار السريع، بالاضافة إلى الروبوتات ذاتية التحكم، والتي تستخدمها الدول الكبرى خاصة في مواجهة الجماعات الارهابية، مثل ما قامت به الولايات المتحدة في أفغانستان والعراق، وقد تم تطوير هذه الآلات تطوير كبير من حيث التقنية ودقة تحديد الهدف والقدرة على الطيران لفترة زمنية طويلة مما أثر على مفهوم المقاتل التقليدي والقوات النظامية في الحروب العسكرية خاصة من حيث الاعتماد على التكنولوجيا ونوعية السلاح مقابل العدد المطلوب من القوة البشرية[٥٦]، وقد توفر تقنيات الذكاء الاصطناعي بعض المزايا على الجانب الأمني والعسكري تتلخص في زيادة وتيرة العمليات العسكرية والأمنية بشكل عام مما يوفر في الوقت ويعجل بتحقيق الهدف، كما تعمل على تعزيز القدرات البشرية في الجوانب الأمنية والعسكرية من خلال تطوير أنظمة أمنية وعسكرية حديثة أقل تكلفة وبقدرات استثنائية، مع تقليل ارتباط القوة الأمنية والعسكرية بحجم السكان وبالقوة الاقتصادية للبلد مما يمكن الدول الصغيرة من رفع كفاءة جيوشها إذا استطاعت الاستفادة من مقومات الذكاء الاصطناعي[٥٧].

ثالثا: ظهور فواعل غير تقليدية تلعب دور أساسي في الساحة الدولية وعلى رأسها شركات التكنولوجيا التي تمتلك تقنيات هذا الذكاء الاصطناعي، والتي سيصبح لها تأثير على الجوانب الاقتصادية والسياسية والأمنية، مما قد يؤثر على مفهوم السيادة الوطنية بالمعنى التقليدي، ويزيد من التدخل في شئون الدول والتأثير على قراراتها.

رابعا: خلق منافسة شديد بين الفاعلين الكبار في مجال الذكاء الاصطناعي من الدول العظمى، ومن أبرزهم الولايات المتحدة وروسيا والصين، حيث حرصت الصين على وجودها في الريادة العالمية في مجال تطوير الذكاء الاصطناعي للعام ٢٠٣٠ من خلال خطة عمل تطويرية أصدرتها عام ٢٠١٧، تعمل من خلالها على توظيف تقنيات الذكاء الاصطناعي من نظم دعم اتخاذ القرارات

(ISSN: 2536 - 9555)

الاستراتيجية بفاعلية وجدوى أكبر، وكذلك في مجال تطوير المركبات العسكرية ذاتية التحكم، وفي المقابل تركز روسيا بشكل أساسي على الروبوتات في مجال تطوير الذكاء الاصطناعي خاصة المجالات الأمنية والعسكرية، أما الولايات المتحدة الأمريكية فقد حرصت على تصميم اطار عمل يهدف إلى الحفاظ على التفوق التكنولوجي للجيش الأمريكي ضد المنافسيين العالميين(٥٨).

الخاتمة

في هذه الورقة، تم تناول نماذج من التهديدات الجديدة في العلاقات الدولية متمثلة في السيبرانية والذكاء الاصطناعي باعتبارهما طفرتين من طفرات الثورة التكنولوجية الحديثة التي أثرت على كافة المجلات ومنها المجال السياسي، وتصاعدت وتيرة استغلال الفضاء السيبراني وتقنيات الذكاء الاصطناعي لفرض قوة الدولة وتحقيق تفوق ونفوذ على الساحة الدولية، وقد أنتج ذلك نوع مختلف من التفاعلات الدولية وأثر على مفاهيم القوة والصراع والحرب، كما أثر على الأدوات المستخدمة لتحقيق القوة وكذلك اللاعبين الدوليين.

وقد استعرضت الورقة البحثية في المحور الأور مفهوم التهديدات الأمنية الجديدة والتي أطلق عليها تهديدات غير تقليدية، أو تهديدات لا تماثلية، والتهديدات الهجين والتي لها طبيعة مختلفة عن التهديدات التقليدية.

أما المحور الثاني من الدراسة فقد ركز على مفهوم السيبرانية وتأثيريها في تفاعلات ومفاهيم العلاقات الدولية وخلصت الدراسة إلى عدة نتائج شملت:

١. تزايد الارتباط بالفضاء الالكتروني الذي اتسع معه خطر الهجمات الالكترونية من قبل الفاعلين في النظام الدولي سواء دولا أو فاعلين من غير الدول.
٢. تصاعد أهمية الشركات العاملة في التكنولوجيا وبروزها كعامل مؤثر في الفضاء الالكتروني خاصة مع امتلاك بعضها تقنيات تفوق قدرة بعض الحكومات.
٣. تغير طبيعة القوة والنفوذ التي لم تعد تقتصر على القوة المادية وإلحاق ضرر على أراضي الخصم في ظل الاعتماد الدولي المتبادل على أنظمة التكنولوجيا في هجماتها وفرض نفوذها.

٤. تصاعد التنافس بين الشركات العاملة في مجال الأمن الالكتروني لزيادة الانفاق على تأمين البنى التحتية السيبرانية للدول مع ظهور فاعلين مختصين بالقرصنة الالكترونية.
٥. تزايد الترابط بين الأمن والتكنولوجيا في ظل تراجع سيادة الدولة لصالحد دور الفاعلين الآخرين، وبالتالي حدوث تغيير في مفهوم القوة الوطنية .
٦. تغير منظور الحرب وتعدد مستوياتها وأنماطها.

وتناول المحور الثالث من الدراسة مفهوم الذكاء الاصطناعي وتأثيره على العلاقات الدولية كنموذج من التهديدات الجديدة التي أفرزت تغيرات على الساحة الدولية وتنبئ بمزيد من التغيرات في شكل وطبيعة التهديدات والحروب، **وقد خلصت الدراسة إلى أن هناك فرص وتحديات شملت ما يلي:**

بالنسبة للفرص؛ تقدم تقنيات الذكاء الاصطناعي فرص التحكم الذاي في التطبيقات الأمنية والعسكرية لتطوير الأداء الأمني للدول تتميز هذه التقنية بقدرتها على القيام بالأعمال الأكثر تعقيدا من الناحية المعرفية والتي تحتاج إلى وقت وجهد بشري كبير جدا ومنها جمع كم هائل من المعلومات وتحليلها والقيام بالعمليات القتالية التي يصعب قيام البشر بتنفيذها، وبالتالي تقلل من المخاطر التي قد يتعرض لها البشر مع خفض التكاليف على المدى البعيد، هذا بالاضافة إلى توفير السرعة والتحكم وبالتالي توفير وتيرة العمليات العسكرية خاصة في المهام طويلة الأمد التي تحتاج فترة زمنية طويلة، مع القدرة على التنبؤ بالأحداث وتحسين نوعية ودلالة المعلومات التي تستنبطها لصانع القرار.

أما التحديات فتتبلور في امكانية حدوث اختراقات وسرقات لتلك التقنية وذلك لاعتمادها على البرمجيات عن طريق المخترقون اللذين يمثلون خطورة في سير عملياتها بشكل صحيح خاصة من حيث تحليل البيانات والتنبؤ، هذا بالاضافة إلى لخطورة المدى التخريبي والخطر الخاص بالأنظمة العسكرية المدعومة بتقنيات الذكاء الاصطناعي التي ستؤثر بشكل كبير على الصراعات الدولية، كما أن عدم كفاية الاتفاقيات والمعاهدات الدولية التي تتعامل مع كافة الجوانب الخاصة بتقنيات الذكاء الاصطناعي، يمثل تحدي هام خاصة أن تلك الاتفاقيات الخاصة

(ISSN: 2536 - 9555)

بالحرب والأسلحة أبرمت منذ وقت طويل وبالتالي لم تتطرق لتلك التقنيات الجديدة.

وفي النهاية توصي الدراسة بأهمية ربط دراسة الفضاء الالكتروني والذكاء الاصطناعي بالقوة والأمن مما يتوجب معه توسيع المنظور الدراسي ليشمل مناهج مفاهيمية من دراسات العلوم والتكنولوجيا (STS) science and technology studies. بهذه الطريقة، يمكن للعلماء الانتباه إلى الديناميكيات والعمليات والممارسات الهامة والجهات الفاعلة غير التقليدية في سياسات وحوكمة الذكاء الاصطناعي والفضاء الالكتروني، وخلق خطاب سياسي أكثر دقة حول مفاهيم التكنولوجيا والأمن.

هوامش ومراجع البحث:

(1) Giegerich, B., 2016. Hybrid warfare and the changing character of conflict. Connections, 15(2) , pp.65-72.

(2) Boege, V., 2006. Traditional approaches to conflict transformation: Potentials and limits.

(3) Sammons, C., 2009. A New Division of Labor: Meeting America's Security Challenges beyond Iraq.

(٤) محمد حمشي، ٢٠١٨ "مدرسة باريس للدراسات الأمنية واشكالية مستوى التحليل في العلاقات الدولية"، مجلة السياسة الدولية، (٢١٢): ٥٣، ص ص ١٧٤-١٨٤.

(5) Nye, J.S., 1990. Soft power. Foreign policy, (80) , pp.153-171.

(6) Mack, Andrew. "Why big nations lose small wars: The politics of asymmetric conflict." World politics 27, no. 2 (1975): 175-200.

(7) Richard H. Ullman, "Redefining Security", International Security, Vol. 8, No. 1 (Summer, 1983) , pp. 129-153

(8) Fleming, B.P., 2011, "Hybrid threat concept: Contemporary war, military planning and the advent of unrestricted operational art", Army command and general staff coll fort leavenworth ks school of advanced military studies.at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a545789.pdf (accessed 11 Jan 2021).

(9) Mattis, L.G.J.N., 2005,"Future Warfare: The Rise of Hybrid Wars", Proceedings Magazine, Vol. 132. At: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf (accessed 11 Jan 2021)

(10) George C. Casey, "America's Army in an Era of Persistent Conflict," Army Magazine (October 2008) , 28

(11) Hoffman, F.G., 2010. 'Hybrid threats': Neither omnipotent nor unbeatable., op. cit.

(12) Hoffman, F.G., 2007. Conflict in the 21st century: The rise of hybrid wars. Arlington: Potomac Institute for Policy Studies.p.51.

(13) Hoffman, F.G., 'Hybrid threats': Neither omnipotent nor unbeatable, op cit.

(14) Adamsky, D., 2015. Cross-domain coercion: The current Russian art of strategy. IFRI Security Studies Center.

(15) Panait, I., 2015, "The Hybrid War Concept-Arguments for and Versus", Research and Science Today, no.3, p.130.

(16) Radin, A., 2017. Hybrid Warfare in the Baltics: Threats and Potential Responses (No. RR-1577-AF). RAND Project AIR FORCE Santa Monica United States.

(17) Patten, B.C. and Odum, E.P., 1981. The cybernetic nature of ecosystems. The American Naturalist, 118(6) , pp.886-895.

(18) Schmeink, L., 2015. 13. CYBERPUNK AND DYSTOPIA: WILLIAM GIBSON, NEUROMANCER (1984). At:https://d1wqtxts1xzle7.cloudfront.net/50829904/13_Schmeink_Gibson_preproof.pdf?1481463128=&response-content-disposition=(acsessed 20 January 2021)

(19) Kuehl, D.T., 2009. From cyberspace to cyberpower: Defining the problem. Cyberpower and national security, 30.

(20) Valeriano, B. and Maness, R.C., 2018. International relations theory and cyber security. The Oxford Handbook of International Political Theory, p.259.

(21) Arquilla, J., and D. Ronfeldt (1993). Cyberwar is Coming! Comparative Strategy 12(2): 141–65

(ISSN: 2536 - 9555)

(22) Held, D., McGrew, A., Goldblatt, D. and Perraton, J., 2000. Global transformations: Politics, economics and culture. In Politics at the Edge (pp. 14-28). Palgrave Macmillan, London.

(23) Gumahad, A.T., 1996. Cyber troops and net war: The profession of arms in the information age (No. AU/AWC/RWP123/97-04). AIR WAR COLL MAXWELL AFB AL.at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a394073.pdf (accessed 21 January 2021)

(24) Klimburg, A., 2011. Mobilising cyber power. Survival, 53(1) , pp.41-60.

(25) Pagallo, U., 2015. Cyber force and the role of sovereign states in informational warfare. Philosophy & Technology, 28(3) , pp.407-425.

(26) Held, D., McGrew, A., Goldblatt, D. and Perraton, J., 2000. Global transformations: Politics, economics and culture. In Politics at the Edge (pp. 14-28). Palgrave Macmillan, London.

(27) Nye, J. S. (2011). Nuclear Lessons for Cyber Security? Op.cit.

(28) Craig, A. and Valeriano, B., 2016, May. Conceptualising cyber arms races. In 2016 8th International Conference on Cyber Conflict (CyCon) (pp. 141-158). IEEE.

(29) Jeremy Rehm, What is the U.S Space Force? Space 10 October, 2018, at: https://www.space.com/42089-space-force.html (accessed at 7 February 2021)

(30) Hanna Samir Kassab,2014, "In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare" in, Jan-Frederik Kremer, Benedikt Müller (eds) , Cyberspace and International Relations: Theory, Prospects and Challenges, (Springer, Berlin, Heidelberg). pp.59-71.

(31) Kshetri, N., 2014. Cybersecurity and international relations: The US engagement with China and Russia. In Proc. FLACO-ISA Joint Conf..

(32) Mumford, A., 2013. Proxy warfare. (Cambridge & Malden: John Wiley & Sons) p8.

(33) Warren, P., Kaivanto, K. and Prince, D., 2018. Could a cyber-attack cause a systemic impact in the financial sector? Bank of England Quarterly Bulletin, 58(4), pp.21-30.

(34) Dunn Cavelty, M. and Wenger, A., 2020. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), pp.5-32.

(35) Alford, L.D., 2001. Cyber warfare: A new doctrine and taxonomy. United States Air Force.

(36) Parks, R.C. and Duggan, D.P., 2011. Principles of cyberwarfare. IEEE Security & Privacy, 9(5) , pp.30-35.

(37) Robinson, M., Jones, K. and Janicke, H., 2015. Cyber warfare: Issues and challenges. Computers & security, 49, pp.70-94.

(38) Salma Shaheen, "Offense–Defense Balance in Cyber Warfare" in, Jan-Frederik Kremer, Benedikt Müller (eds) op.cit, pp.82-83.

(39) I bid.

(40) Sascha Knoepfel, "Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War", in Jan-Frederik Kremer, Benedikt Müller (eds) , op.cit, pp.117-124.

(41) Maurer, T., 2016. 'Proxies' and Cyberspace. Journal of conflict and security law, 21(3) , pp.383-403.

(42) Dunn Cavelty, Myriam, and Jonas Hagmann. "The Politics of Security and Technology in Switzerland." Swiss Political Science Review 27, no. 1 (2021): 128-138.

(43) McCarthy, John, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon. "A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955." AI magazine 27, no. 4 (2006): 12-12.

(44) Kurzweil, Ray, Robert Richter, Ray Kurzweil, and Martin L. Schneider. The age of intelligent machines. Vol. 580. Cambridge: MIT press, 1990.

(45) Brynjolfsson, Erik, and Andrew McAfee. The second machine age: Work, progress, and prosperity in a time of brilliant technologies. WW Norton & Company, 2014.

(46) Greg Allen & Taniel Chan, Artificial Intelligence and National Security, (Harvard Kennedy School; Belfer Center for Science and International Affairs, 2017) p.7.

(ISSN: 2536 - 9555)

(47) Graßmann, Carolin, and Carsten C. Schermuly. "Coaching with artificial intelligence: concepts and capabilities". Human Resource Development Review 20, no. 1 (2021): 106-126.

(48) Buchanan, Ben. "A National Security Research Agenda for Cybersecurity and Artificial Intelligence". Center for Security and Emerging Technology Issue Brief (2020): 7.

(49) Amicelle, A., C. Aradau and J. Jeandesboz (2015). Questioning Security Devices: Performativity, Resistance. Politics. Security Dialogue 46(4): 293–306.

(50) Greg Allen & Taniel Chan, op cit, p.16.

(51) Allen, Gregory, and Elsa B. Kania. "China is using America's own plan to dominate the future of artificial intelligence." Foreign Policy 8 (2017).

(52) Ibid.

(53) Cummings, M.L., Roff, H.M., Cukier, K., Parakilas, J. and Bryce, H., 2018. Artificial Intelligence and International Affairs. Chatham House Report, pp.7-18.

(54) Jacob Parakilas and Hannah Bryce, "Introduction: Artificial Intelligence and International Politics", in: M. L. Cummings, Heather M. Roff, Kenneth Cukier, Jacob Parakilas and Hannah Bryce, Artificial Intelligence and International Affairs Disruption Anticipated, (Chatham House, the Royal Institute of International Affairs, 2018) pp:1-7

(55) Scharre, P. (2017) , 'A security perspective: Security concerns and possible arms control approaches', in United Nations Office for Disarmament Affairs (UNODA) (2017) , Perspectives on Lethal Autonomous Weapons Systems, UNODA Occasional Papers – No. 30, November 2017, New York: United Nations, https://www.un.org/disarmament/publications/occasionalpapers/unoda-occasional-papers-no-30-november-2017/, pp. 19–33.

(٥٦) كمال دحماني, ٢٠٢٠. الوضع القانوني للطائرات المسلحة من دون طيار في القانون الدولي الإنساني. دائرة البحوث والدراسات القانونية والسياسية, ٤(٨), .pp.39-68.

(٥٧) حسن يوسف أبو منصور،٢٠٢٠، "الذكاء الاصطناعي وأبعاده الأمنية"، أوراق السياسات الأمنية، ١ (١).

(٥٨) المرجع نفسه.