

الامن السيبراني في ظل الذكاء الاصطناعي (التهديدات ، الفرص والتحديات) Cybersecurity in the age of artificial intelligence (threats, opportunities and challenges)

والي فايذة * استاذ محاضر ب

جامعة المسيلة – الجزائر

عضوة بمخبر العلوم السياسية الجديدة جامعة المسيلة

البريد الإلكتروني fayza.ouali@univ-msila.dz

تاريخ النشر: 2026/06/10	تاريخ القبول: 2026/06/09	تاريخ الارسال: 2026/04/25
-------------------------	--------------------------	---------------------------

ملخص :

إنه في خضم الاحداث والمستجدات الدولية والاقليمية ذات الأبعاد التكنولوجية وجد الذكاء الاصطناعي موقعه في جل المجالات البحث العلمي. الطب. الاقتصاد والامن السيبراني سواء الدفاع او الهجوم. ويعد كل من الذكاء الاصطناعي و الأمن السيبراني من صور ومظاهر التطور التكنولوجي الهائل الذي نعيشه منذ سنوات واكتسبا هذان المجالان و الميدانان شهرة واسعة النطاق في التكنولوجيا الحديثة وذلك راجع لأدوارهما الهامة في تشكيل العالم الرقمي فقد حرصت المؤسسات على الاستعانة بأدوات و أنظمة الامن السيبراني التي تعمل بالذكاء الاصطناعي حتى تتمكن من اكتشاف التهديدات و الاستجابة لها بشكل أسرع.

وهو ما جعل هذه الدراسة تستهدف العلاقة بين الذكاء الاصطناعي والامن السيبراني وابرار التحديات والفرص والتهديدات التي نجرت عن هذه العلاقة .

الكلمات المفتاحية: الذكاء الاصطناعي؛ الأمن السيبراني؛ الفضاء السيبراني؛ الامن القومي .

*المؤلف المرسل : والي فايذة

Abstract:

It is amidst international and regional events and developments with technological dimensions that artificial intelligence has found its place in most fields of scientific research, medicine, economics and cybersecurity, whether defensive or offensive. Both artificial intelligence and cybersecurity are among the forms and manifestations of the tremendous technological development that we have been experiencing for years, and these two fields have gained widespread fame in modern technology due to their important roles in shaping the digital world.

Institutions have been keen to use cybersecurity tools and systems that operate with artificial intelligence in order to be able to detect threats and respond to them more quickly.

This led this study to focus on the relationship between artificial intelligence and cybersecurity, highlighting the challenges, opportunities, and threats arising from this relationship, and the uses of artificial intelligence in cybersecurity strategies.

Keywords:Artificial intelligence; cybersecurity; cyberspace; national security

مقدمة:

يشهد النظام الدولي المعاصر تحولا بنويا في المفاهيم القوة والأمن، فرضته الثورة التكنولوجية الرابعة وما صاحبها من تمدد للبيئة الرقمية في كافة مفاصل الدولة الحديثة. ولم يعد الفضاء السيبراني مجرد ساحة خلفية للتبادل المعلوماتي. بل استحال إلى مسرح استراتيجي تتشكل فيه موازين قوى جديدة بفعل الذكاء الاصطناعي فهو متغير وافد استطاع تغيير قواعد وتكتيكات الدفاع والهجوم. تتجاوز التكتيكات والقواعد التقليدية على مستوى التعقيد الدقة والسرعة الناجمة عن عنصر بشري.

فاهتمام دوائر الدراسات الاستراتيجية لم يتمحور في مزايا الذكاء الاصطناعي بل شمل العلاقة بينه وبين الأمن السيبراني على مستوى الدول او النظام الدولي شاملا للابعاد المفاهيمية والنظرية .

تأسيسا على ماسبق تسعى الدراسة وفق منهج وصفي الإحاطة بمتغيرات الدراسة و الظاهرة ومعرفة ماهيتها بالإضافة للمنهج التحليلي الذي سنستند عليه في الكشف عن مدى تأثير استخدامات الذكاء الاصطناعي على استراتيجيات الامن السيبراني والتحديات التي فرضت على مستوى الامن السيبراني للدول وكذا امنها القومي و على طبيعة التهديدات المواجهة جراء تقنيات الذكاء الاصطناعي وهذا مايستوجب اطار نظريا نكشف من خلاله مدى نجاعة الأطر النظرية في تحليل ما اضافته الذكاء الاصطناعي وعلاقته بالامن السيبراني على مستوى التهديدات المفروضة و التحديات المطروحة و الفرص المتاحة على مستوى استراتيجيات الامن القومي و السيبراني دفاعا و هجوما

وعليه فان الدراسة ستناقش المشكلة البحثية المتمحورة حول التحديات التي قرضها الذكاء الاصطناعي على الامن السيبراني و الامن القومي للدول وكيف اثرت البيئة الرقمية على طبيعة التهديدات وسبيل مواجهتها في ظل تعقيدات التي فرضها الذكاء الاصطناعي على

مستوى الامن السيبراني للدول سواء الأهداف او الفواعل و تكتيكات استراتيجيات الدفاع والهجوم .

المحور الأول: مفاهيم عامة حول لأمن السيبراني والذكاء الاصطناعي

إن الولوج لتكوين رؤية معرفية حول الفضاء السيبراني يستوجب ويسلزم وضع لبنة مفاهيمية وتفكيكها لكل من الامن السيبراني و الذكاء الاصطناعي بوصفهما ركيزتين للانتقال من الأطر الدفاعية و الهجومية التقليدية الى الحديثة الذكية ، هذا ما يفرض ضبط المصطلحات المتحورة حول البيئة الرقمية الدكاء الاصطناعي و الامن السيبراني وهي خارطو مفاهيمية تعد مدخلا للاستعاب ديناميكات العلاقة بين هدة المصطلحات .

الفرع الأول: المقصود بالامن السيبراني

على العموم والمعروف أن الأمن السيبراني مصطلح يشير على أن الأنظمة و الشبكات و البرامج و المواقع الجغرافية لها حماية من أي هجمات سيبرانية رقمية ومحمية من أي عائق أو هجمات الكترونية تحول دون أداء مهامها . فهذه الهجمات عادة ما تهدف لاختراق الانظمة في سبيل الوصول الى المعلومات الحساسة لتغييرها او إتلافها أو للابتزاز خاصة المالي . فهو أمن الشبكات و الأنظمة المعلوماتية ، و البيانات و المعلومات و الأجهزة المتصلة بالأنترنت .

وقد طرح إدوارد أمورسو Edward Amoroso صاحب كتاب الامن السيبراني 2007 على أنه " وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات "، وتشمل تلك الوسائل الأدوات المستخدمة في كشف الفيروسات ووقفها وتوفير الاتصالات المشفرة ومواجهة القرصنة لحماية البيانات .¹

وعرفته منى جبور " أنه النشاط الذي يؤمن حماية الموارد (البشرية و المالية) المرتبطة بتقنيات الاتصالات و المعلومات ويضمن إمكانيات التغلب على الخسائر و الأضرار التي تترتب في حال تحقيق مخاطر وتهديدات ، كما يتيح إعادة الوضع إلى ماكان عليه بأسرع وقت"²

الفرع الثاني المقصود بالذكاء الاصطناعي وتطبيقاته المؤثرة على الأمن القومي

أولا: مفهوم الذكاء الاصطناعي

يعرف الذكاء الاصطناعي عملية محاكاة للذكاء البشري وطريقة عمله بواسطة الآلات خاصة أجهزة الكمبيوتر، كالقدرة على التفكير والاستكشاف، فمع التطورات الهائلة للحواسيب يتجلى استطاعتها أداء مهام معقدة حيث يمكنه الاستكشاف وإثبات النظريات الرياضية المعقدة... الخ ويتميز بسرعة الانجاز مع دقة عالية. وهناك تطبيقات تمكن من

مضاهات مستوى أداء الخبراء و المحترفين بالقيام بمهام محددة ومن هذه التشخيص الطبي، محركات البحث والقررة على العرف على الصوت و الكتابة اليدوية³.

عرف الذكاء الاصطناعي أنه الكيفية و الآلية التي يتم من خلالها محاكاة قدرات الذكاء البشري. وهو جزء من علم لحاسوب الذي يتعامل مع عملية تصميم الأنظمة الذكية التي تظهر مجموعة من الخصائص التي يتم ربطها بالذكاء المتعلق بالعديد من السلوكيات البشرية.⁴

ثانيا : تطبيقات الذكاء الاصطناعي على مجالات الامن القومي

لا شك أن التطورات التقنية الحاصلة لا سيما الذكاء الاصطناعي واستخداماته، له تأثير على مجالات حيوية تمس الامن القومي للدولة كالأمن ، الدفاع، الطب، الاقتصاد و السياسة الخارجية ، الوظائف الخدمية للدولة وغيرها . ففي الامن و الدفاع يؤثر استخدامه في الارتقاء بمستوى القدرات الاستخباراتية و المراقبة والتحليل وتوقع التهديد و الاستجابة السريعة و رد الفعل وتحليل البيانات الضخمة ومنه فانه يخفض من التهديدات و المخاطر الداخلية و الخارجية . إن هذا ما يساهم في تعزيز وحماية الامن القومي.⁵

أما بالنسبة لمجال الطب في استخدامات الذكاء الاصطناعي يساهم في تعزيز الصحة العامة وبالتالي الامن الصحي بشكل عام ، ويتجلى مثلا في مواجهة الأوبئة بفعالية . وفي ميدان الاقتصاد فإنه يمكن من يعتمد على الذكاء الاصطناعي في تحليل البيانات واتخاذ القرارات الاستراتيجية و تحسين إدارة الأزمات المالية وهو ما يساهم في تحقيق الاستقرار الاقتصادي وتعزيز الأمن الاقتصادي⁶

الفرع الثالث: مفهوم وخصائص البيئة السيبرانية

أولا: مفهوم البيئة الرقمية (الفضاء الرقمي)

ما يمكن طرحه للاحاطة بمفهوم البيئة السيبرانية (الرقمية) انها بيئة وفضاء رقمي أساسه أنظمة الكمبيوتر وكذا شبكة الانترنت كما تشمل البيانات الرقمية و المعلومات⁷. وهو ما اتجه نحوه تعريف الاتحاد الدولي للاتصالات لها انها مجال مادي ولا مادي يتشكل من نتاج عناصر تتمثل في أجهزة الكمبيوتر. الشبكات , البرمجيات و رقمنة وحوسبة البيانات . المحتوى . معطيات النقل و التحكم . ومستخدموا كل هذه العناصر السالفة الذكر.⁸

من خلال هذا التعريف نستطيع القول انه يمكن تبنيه كتعريف للفضاء السيبراني حيث لم يتجاهل العنصر البشري عكس التعريفات التقنية نذكر منها تعريف الوكالة الفرنسية لأمن أنظمة الإعلام الذي اعتبره محيط تواصل مكون من خلال الربط البيئي العالمي لوسائل المعالجة الألية للمعطيات الرقمية⁹.

ثانيا : خصائص البيئة السيبرانية وعلاقتها بالأمن القومي

أول خاصية هي اللاتيقين، إن عدم القدرة على فهم طبيعة التهديدات و غموضها مع غموض وعدم وضوح النوايا من طرف الفواعل مع الصعوبة في قياس حجم المخاطر و الضرر في الفضاء الرقمي فان ذلك يحمل دلالة على اللاتيقين في البيئة السيبرانية ما يحد ويؤثر على قدرة الدولة على حماية امنها القومي ويربك دفاعها وخططه وبنيتها التحتية الحيوية في خطر¹⁰. إن هذه الخاصية تؤدي لعدم القدرة على تحديد هوية الفاعل بدقة ما يعيق اتخاذ القرار بسبب عدم الجزم بالجهة المعتدية ما يضعف سياسة الردع و يؤدي لفجوة أمنية متعلقة بالفضاء السيبراني ما يوضح جليا الخاصية الثانية المتمثلة في صعوبة الاسناد¹¹.

ومن بين الخصائص نجد ان البيئة الرقمية هي بيئة لامادية تعتمد على البيانات و المعلومات و الأنظمة الرقمية لذا اصبح حماية الامن القومي معقدا لان التهديدات لا تتعلق بالحدود او الأراضي، ان هذا ما يؤدي الى وجود خاصية أخرى للبيئة الرقمية أو الفضاء السيبراني وهي تجاوز المدى الجغرافي فالتهديدات الرقمية غير مقيدة بحدود الدول ويلزم الدول على التعاون لحماية أنظمتها وهنا يتبين ارتباط الامن القومي بأمن الفضاء الرقمي . هذا في ظل خاصية السرعة التي تتميز بها الهجمات السيبرانية ما قد يمثل تهديدا للدولة خصوصا اذا كان الهدف قطاعات حيوية ما قد يسبب شلل على مستواها، ومنه يمكن القول ان حجم التهديدات و انعكاساتها الوخيمة نجد انه تم بتكلفة بسيطة مما يبيح لفواعل واطراف صغير دولية او غير دولية أن تهدد دول كبرى ما من شأنه أن يؤثر على ميزان القوة التقليدي ويجعل الأمن القومي اكثر هشاشة امام الفواعل من غير الدول¹²

المحور الثاني: الاطار التحليلي والنظري للعلاقة بين الذكاء الاصطناعي والأمن

السيبراني

إن ما يثير الخوض في هذا المحور هو التساؤل عن مدا موائمة مبادئ النظريات مع الفضاء السيبراني مخرجاته ومنها الذكاء الاصطناعي .

إن المجال السيبراني ونطاقه يجعل بما كان النظر انه أضحى ساحة للقوة لها من المميزات تجعلها ترقى لمستوى أن تكون تحدياً في العلاقات الدولية الناجمة عن خصوصية الفضاء السيبراني نتيجة تعدد الجهات الفاعلة.¹³ فالفضاء السيبراني يعد بيئة رقمية تفاعلية حتى انه أصبح الذراع الرابع للجيش الحديثة. حيث اقبلت عدة دول في استخدامه في المجال الأمني والعسكري بهدف تحقيق تقدم وتطور في الميدان السياسي والعسكري¹⁴.

وفي هذا السياق يمكن أن نستخلص ونستشف رؤية المنظور الواقعي لمتغيرات الذكاء الاصطناعي وما فرضه من تحولات على مستوى العلاقات الدولية و الامن السيبراني للدول . ومن المعلوم ان النظرية الواقعية من اعرق النظريات و تركز اهم مبادئها ؛لتقليدية على متغير(القوة ، المصلحة، فوضوية النظام الدولي ، الدولة كفاعل رئيس في العلاقات الدولية) كما ارتكزت على ميزان القوى مع كينيث والتز.

فبالنسبة للطابع الفوضوي في العلاقات الدولية فالواقعية ترى أنه يتلائم مع البيئة السيبرانية التي تتميز باللايقين فالتحديات التقليدية للدول تستخدم إخفاء الهوية في الفضاء والبيئة الرقمية لعبور الحدود افتراضيا دون نتائج واثار قانونية او دبلوماسية فمن الصعب كشف الهوية و تحميل المسؤولية . ومنه يكون هناك عدم استقرار على مستوى التوازن الهجومي و الدفاعي ما يؤدي لخلق سياق من الصراع في الفضاء السيبراني.¹⁵

وفيما يخص تأثير الذكاء الاصطناعي والامن السيبراني فانه اصبح بيئة تتعدد فيها الفواعل وتتفاعل فيما بينها من دول وشركات تكنولوجيا ، الهاكرز جماعات ناشطة ، جماعات إرهابية ، شركات خاصة بالامن السيبراني ...الخ وهي جميعها اطراف تتفاعل بطرق متجدد ومتغيرة وصعبة التنبؤ بها. ومنه يمكن القول ان تبني الواقعية للدول كفاعل ولاعب وحيد بسبب إحتكارها للسلطة يواجه تحديا في الفضاء السيبراني.¹⁶

ومن جهة أخرى متغير القوة الذي يعد من متغيرات هذه النظرية، قد حصرتها الواقعية خصوصا الواقعية التقليدية في القوة العسكرية أو الصلبة ما يجعله مفهوما يحتاج الى التوسيع فهو لم يعد مقتصرًا على القوة الصلبة بل أصبحت القوة الناعمة و الرقمية جزءًا أساسيا . وأيضا صار الذكاء الاصطناعي أداة للدردع الرقمي.

وفيما يخص المنظور الليبرالي الذي يفترض أن الديمقراطية والتجارة المتبادلة تقلل من احتمالية الحروب وهو ما جعل رواد المنظور الليبرالي الجديد يطورون مفهوم القوة

الناعمة مؤكدين على فاعلية المؤسسات الدولية في تعزيز التعاون وتقليل النزاعات من خلال الاعتماد المتبادل . غير أن التحدي الذي يواجه الليبرالية هو حوكمة التكنولوجيا العابرة للحدود اذ انه اصبح هناك حاجة لوجود مؤسسات دولية لتنظيم الذكاء الاصطناعي تحاكي لاتفاقية المناخ بباريس وكذا اتفاقيات التجارة¹⁷

وجاء البنائية و التي بنيت على كيفية بناء الواقع الاجتماعي عبر الأفكار الهويات الدين اللغة التي تعد معايير لتشكل التصورات حول التهديدات أو التحالفات من هذا الطرح قد أكد أونوف على دور اللغة في بناء القواعد الدولية ، وعصر الذكاء الاصطناعي تكتسب البنائية أهمية أكبر حيث ان الذكاء الاصطناعي و الفضاء السيبراني أداة لبناء هويات رقمية كالخوارزميات وداواتها كوسائل التواصل الاجتماعي التي تعد الية تؤثر على المدركات الجماعية ومنه فالذكاء الاصطناعي يعيد تشكيل الهويات الوطنية أو الفرعية او العابرة للحدود او حتى نشوء هويات افتراضية تتجاوز الجغرافيا¹⁸

ان البنائية تركز إذن للتركيز على المساهمة في ظل الفضاء الرقمي لتوسيع مجال المفاهيم و التعريف، و تحويل القيم ما يحدث تغيرات على مستوى الواقع الاجتماعي . وبالتالي تحديد بعض الأنشطة على أنها تهديدات ليست مبنية على مادي بل تفسير ذاتي مشترك للمجال أي مجال التعريف. لاسيما ان الطرح البنائي يشتمل أيضا على تعدد الفواعل في الفضاء الرقمي¹⁹

مما يطرح إشكالات تتعلق بتهديدات تمس وجود الدولة وكذا تحدي السيادة الرقمية و التي تتعلق بقدرة ممارسة الدولة التحكم و السيطرة على بياناتها الرقمية و البنية التحتية و البرمجيات لضمان امنها القومي و السيبراني واستقلاليتها ضمن الفضاء الرقمي فضلا عن عدم التبعية التكنولوجية الأجنبية وهو ما يجعل السيادة الرقمية اساسا للامن في ظل عصر التحولات التكنولوجية و الذكاء الاصطناعي .

المحور الثالث: الذكاء الاصطناعي وانعكاساته على الامن السيبراني للدول

لقد اصبح الامن السيبراني في ظل استخدامات الذكاء الاصطناعي متغير محوري في العقيدة الأمنية للدول وعليه تم الانتقال من اطر ومرحلة الامن الكلاسيكي الى السيادة الرقمية و عصر الخوارزميات هذا التحول الذي فرض واقعا معقدا .

الفرع الأول: : تأثير الذكاء الاصطناعي على طبيعة التهديدات الأمنية السيبرانية

هناك علاقة وطيدة بين الذكاء الاصطناعي و الأمن السيبراني بشكل عام، إذ يتم تطوير أنظمة الذكاء الاصطناعي التي يمكن استخدامها لتعزيز الأمن السيبراني ، إلى جانب تنفيذ تدابير أمنية لحماية أنظمة الذكاء الاصطناعي من الاختراق و التلاعب .

فبعد تزايد الجرائم السيبرانية لجأت الدول والمؤسسات على اتخاذ وسائل لمكافحة

التهديدات الامنية .فهناك من استعانت بفرق الأمن السيبراني المؤهلة و المدعمة بأحدث تقنيات منها تقنيات الذكاء الاصطناعي حيث انه يعمل ايضا على انشاء تطبيقات أمنية بشكل افتراضي ، تقضي على نقاط الضعف و القوة وتزيد من الدقة في اكتشاف المشكلات وتسريع التحقيقات وامتته أليات الاستجابة²⁰.

إن انتشار انترنيت الاشياء أفرزات ناتجة عن الذكاء الاصطناعي وتطبيقاته واستخداماته أدى الى تنامي التهديدات المحيطة بالافراد، الدول و المنظمات، و الاجهزة بقطاعات حساسة هذا ما يمكن من أن تتعرض لهجمات بوسائل متطورة بتطور التكنولوجيا، ما يؤكد على أن قدرة الانظمة العسكرية الهجومية أو الدفاعية تتطور فمن الناحية الهجومية يصعب الذكاء الاصطناعي من تحديد هوية المنفذ ، أو التنبؤ بالهجوم والدقة في تحديد الأهداف المراد الهجوم عليها اما الدفاعية فيساهم في تقليل مخاطر الهجمات من خلال عمليات مراقبة الشبكات وتحديد التهديدات بسرعة²¹.

لقد صار بإمكان الفواعل الحاق الضرر بالخصم أو العدو او المنافس وتكبيد خسائر كبيرة عبر شل البنية المعلوماتية و الاتصالية أو من خلال التلاعب بالبيانات الاقتصادية و المالية وتزييفها او مسحها من الحاسوب ، وذلك عبر فيروسات تنشر بالحاسب الألى لتنتشر بجميع الحواسيب .وبالتالي فالخسائر ونتائج تلك الهجمات على المستوى الامني الاقتصادي و الاجتماعي جسيمة خاصة اذا مست مؤسسات وإدارات وقطاعات حساسة بالدولة. ومع التطورات التكنولوجية وانظمة الشبكات وبالنظر الى تعدد التهديدات عبر ضم التهديدات السيبرانية اصبح هناك خوف وتوجس من أن يصبح الفضاء الرقمي ذا طابع عسكري فعلي

يسوده تجاوزات لايمكن السيطرة عنها أمام الدخول بسباق نحو التسليح الرقمي كتطوير أسراب تادرونز الطائر ، مادفع بالكثير من 22 دولة بناء قدرات هجومية رقمية في اطار لعبة حرة متزايدة الخطورة على اساس الدفاع المشرع عن النفس و المعاملة بالمثل من الناحية الاستراتيجية إذ أن استخدام نظام تكنولوجيا المعلومات و الاتصالات معلن بوضوح في مذاهب ذات الصلة كوسيلة لتحقيق اهداف عسكرية وسياسية وهو ما لا يمكن استبعاده²².

إن احد التهديدات جراء استخدام تقنيات الذكاء الاصناعي هو توظيفه من طرف فواعل من غير الدول وغير نظامية منها داعش التي طورت من الدرونز واستخدامها بحمل المتفجرات لهو دليل واضح ، إذ إنه استفاد من توفر تكنولوجيا الدرونز المدنية المتاحة للاستخدامات التجارية وقام بتطويرها لحمل متفجرات أو الاستفادة منها في عمليات المراقبة والتجسس و تحديد الاهداف ونفس الامر ينطبق على السيارات المسيرة²³، كما ان تقنيات الذكاء الاصطناعي اصبحت تستخدم في عمليات الاغتيال كمحاولة اغتيال الرئيس الفنزويلي غير انه مع الرونر وتطور تقنية التعرف على الالوجه تصبح فيها عمليات الاغتيال اكثر دقة. واحتمالية اختراق نظم الذكاء الاصطناعي من خلال الهجمات السيبرانية مما يمكن من الجهة المهاجمة ان تسيطر على احد الانظمة والروبوتات العسكرية و اعادة توجيهها مما يترتب عليه اضرار بالمنشآت²⁴. ايضا امكانية خداع نظم الذكاء الاصطناعي فهناك اتجاه نحو الاعتماد على الذكاء الاصناعي في تحديد ورصد التهديدات التي تحدى بالامن القومي للدولة و التنبؤ بالتحويلات التطورات التي يكن ان تحدث حول العالم كا الثورات و الاضطرابات الاجتماعية . غير نجاح طرف معادي في تحديد ورصد عمل تلك الاجهزة فإنه يمن خداعها بمعطيات مزيفة لتتوصل الى نتائج خاطئة وبالتالي مثلا يمكن خداع انظمة التسليح العسكري المستقلة لاتخاذ قرارات خاطئة و اختراق المجتمعات حيث يمكن لدولة اجنبية استخدام نظم الذكاء الاصطناعي لمعرفة التوجهات السياسية والاجتماعية لافراد الدولة المناوئة لها على مواقع التواصل الاجتماعي ومحاولة الربط بين الجماعات المنعزلة جغرافيا و التي تتبنى توجهات مشابهة لهاودعمهم لتبني مواقف سياسية مبينة تضر بمصلحة الدولة و أمنها القومي²⁵.

الفرع الثاني : الذكاء الاصطناعي وانعكاساته على منظومة الأمن والدفاع السيبرانية

بفعل التطورات التكنولوجية و المعرفية و الرهانات الأمنية المستجدة الخ اصبح الفضاء الالكتروني نطاقا للتفاعلات الدول تستخدم فيه تقنيات الذكاء الاصطناعي في أنظمة

التسلح واختراق المؤسسات حساسة وكذا أنظمة التسلح و التي تقوم بتنفيذ مهمتها دون تدخل بشري بناء على معايير الاستهداف المبرمج مسبقا فالواقع الرقمي فرض انماط تفكير اسراتيجي عقيد قتالية تتواءم معه و المعتمد على البيانات الضخمة التي لها قدرات فائقة في الادراك و اتخاذ القرار وهو ما جعل الدول المتقدمة تكنولوجيا ومعلوماتيا تهتم بالذكاء الاصطناعي كولايات المتحدة لا سيما مع تعدد مجالات استخدامات الذكاء الاصطناعي كما عزز الذكاء الاصطناعي القدرات العسكرية على المستوى التشغيلي من خلال الاستشعار عن بعد والإدراك اللحظي والمتغيرات واتخاذ القوانين تحت الضغط اما على المستوى التكتيكي في صنع القرار فسيتم التمكن من أنظمة القيادة المعززة بتكنولوجيا الذكاء الاصطناعي من حيث العديد من أوجه القصور الملازمة لعملية اتخاذ القرارات الاستراتيجية او القدرة على اتخاذ القرار بشكل سريع فوري تلقائي بناء على معلومات دقيقة تجنبها الاخطاء السيبرانية²⁶.

بركار انه اذا أراد قراصنة الانترنت اختراق فقاعة الذكاء الاصطناعي التي تحمي المستخدم فلن تكون مراقبة عاداته الرقمية كافية وحدها بل سيحتاجون أيضا الى مراقبة هذا المستخدم جسديا لمعرفة ادق خصوصياته، وأوضحت ان الذكاء الاصطناعي ليس تقنية جامدة فهو يتعلم في الوقت الفعلي ويتطور باستمرار بناء على البيانات التي يتلقاها ومن ثم فإننا نحتاج الى اجراء تحليلات لملايين التهديدات المحتملة التي تحدث كل يوم، لان الذكاء الاصطناعي يقوم بتحليلها باستمرار ويعمل على اتمتة الاستجابة الأمنية المناسبة لها، وهو ما يحول النظام الأمني في نهاية المطاف الى أداة استباقية. واختتمت بركار مقالها بالقول ان العصر الذي كانت فيه الأجهزة الموثوقة وكلمات المرور المكونة من 10 حرف كافية لضمان الامن قد انتهى، وينبغي علينا ان نبتكر تقنيات قادرة على التكيف بسرعة مثلما تتغير نماذج العمل على نحو متزايد تتغير كذلك الأساليب والتكتيكات التي يتبعها قراصنة الانترنت لاختراقه²⁷

الخاتمة:

تأسيسا خلصت الدراسة لبلورة زاوية نظر مركبة لتوضيح العلاقة بين الذكاء الاصطناعي و الامن السيبراني في البيئة الرقمية والتفاعلات التي طرحت في منظومة العلاقات الدولية. لذا يمكن الوصول لصياغة نتائج تحليلية عملية ونظرية أهمها ما يلي:

1- بروز الذكاء الاصطناعي كمتغير أعاد صياغة رؤية مفاهيمية للأمن بفعل البيئة الرقمية من نظرة تقليدية الى نظرة منطقية افتراضية وقد بلور الذكاء الاصطناعي مفاهيم الدفاع و الاستجابة فحول الامن السيبراني من مقاربة رد فعل الى تنبؤ الاستباقي القائم على الاتمة الذكية . كما أدى لظهور السيادة الرقمية. فالذكاء الاصطناعي قد يكون مضاعفا لقوة الدولة او يعتبر ثغرة في السيادة للدول المفتقرة للتكنولوجيا المحلية ما يجعلها في حالة تبعية رقمية للقوى الكبرى.

2- نظريا يُلاحظ أن هناك قصور في تفسير الفوضى الرقمية إذا لم يتم اعتبار المعضلة الأمنية الرقمية ضمن متغيرات المنظور الواقعي . كما برزت حتمية بناء نظام قيبي أخلاقي دولي ينظم سلوك الفاعلين وهو ما يفرضه الاعتماد المتبادل . وهو الذي برز في الطرح الليبرالي والبنائي.

3- الذكاء الاصطناعي كرس من المعضلة الأمنية لا سيما في البيئة الرقمية فكلما طورت دول أنظمة دفاعية ذكية زاد ذلك في ابتكار دول أخرى أسلحة سيبرانية مضادة أكثر تعقيدا ومنه الدخول في سباق نحو تسليح رقمي

4- ان الصراعات الدولية يمكن مستقبلا ان تدار عبر وكلاء الاذكاء, لذا من المحتمل ان تنتقل المواجهة الى صراع للإرادات الرقمية ومنه فالتحدي مستقبلا هو حوكمة دولية للذكاء الاصطناعي السيبراني ليعطي صيغة قانونية لاستخدام التقنيات في النزاعات المسلحة , ووضع قيود قانونية واخلاقية تقي من الانجرار نحو سباق تسليح رقمي .

5- تحول طبيعة الفاعلين الدوليين حيث تراجعت نسبيا احتكار الدولة للقوة حيث أن الفواعل من غير الدول (الشركات التقنية الكبرى /الجماعات السيبرانية, التنظيمات دون الدول ...الخ لها قدرات توازي قدرات الدول بفعل الذكاء الاصطناعي

6- وجوب دمج الذكاء الاصطناعي في العقيدة الأمنية للدول فقد اصبح امنا وجوديا للدولة لارتباطه بسلامة القطاعات الحيوية (طاقة ,اقتصاد , المنظومات العسكرية

- 752

²⁵ديار محمد الأمين و بابو جمال الدين ، تداعيات الذكاء الاصطناعي على الامن القومي، journal of private law ، المجلد 2 (العدد 1) ، جوان 2024، جامعة زيان عاشور الجلفة، ص 104- 106

²⁶دليلة العوفي،

²⁷سعيد خليل . بن مهدي مرزوق ، الذكاء الاصطناعي كتوجه حتمي في حماية الامن السيبراني ، دراسات في حقوق الانسان ، المجلد 06(العدد جوان 2022)