مجلة رسالة الحقوق

السنة الرابعة عشرة 2022 لشهر آب
العدد الخاص بالمؤتمر القانوني الدولي الثاني
لكلية القانون/جامعة المثنى بالتعاون مع كلية القانون جامعة كربلاء
وكلية القانون جامعة وارث الانبياء(ع) والمنعقد بتاريخ 2022/7/20

دور تقنيات الذكاء الاصطناعي والتشريعات في التصدي للاحتلال الرقمي.

The role of artificial intelligence technologies and legislation in addressing digital occupation.

بحث مقدم من قبل
م.م. حسين عباس حميد
كلية الصفوة الجامعة

الخلاصة.

في ظل التقدم الكبير الذي رافق العالم التقني، فدخلت التقنية وتطبيقاتها لجميع أوجه النشاطات، فالعقل الحصيف والمنطق القَويم يقر بان التقدم التِقني وخاصة في المجال استهداف البنى التحتية الحرجة للدولة تمثل خطورة من اللازم التصدي لها ومواجهتها بكل السبيل والامكانيات التقنية والتشريعية، تُعد اليوم الحرب الرقمية والاحتلال الرقمي احدى نتاجات العصر الحديث وتطوره، فاستخدمت الدول بمؤسساتها الخاصة التي تكونها في سبيل احتلال والتجاوز على الدول الأخرى بصورة أكبر واوسع، وعلى الرغم من أن الكثير من دول العالم شرعت القوانين ووضعت الأجهزة التقنية المختصة التي تواجهه إلا ان هذا التوجه متوسع يومًا بعد يوم بسبب وجود الثغرات وعدم تحديث الاستراتيجيات، لذا يجب ان تكون هنالك مَصدات لمواجهته والحد منه بصورة محدثة، وخاصة في ظل عالم رقمي جديد.

الكلمات المفتاحية: الذكاء الاصطناعي- العالم الرقمي- الإرهاب الرقمي- الاحتلال الرقمي- المواجهة الجنائية.

Abstract.

In light of the great progress that accompanied the technical world, technology and its applications entered all aspects of activities . the prudent mind and sound logic acknowledge that technical progress, especially in the field of targeting the critical infrastructure of the state, represents a danger that must be addressed and confronted by all means and technical and legislative capabilities. Today, it is considered digital war and occupation . Digital is one of the products of the modern era and its development , so countries used their own institutions that they formed in order to occupy and transgress other countries in a larger and wider way , and although many countries of the world have legislated laws and put in place specialized technical devices that confront it, this trend is expanding day after day due to the presence of loopholes and not updating strategies.

Key words: The role , artificial intelligence, technologies , legislation , addressing digital occupation.

المقدمة.

بعد انتهاء الحربين العالميتين وما خلفتهما من آثار وخسائر بشرية ومادية، بدأت الدول بالبحث عن وسائل وأساليب أخرى للقتال من شأنها أن تحقق لها الميزة العسكرية على الخصوم، ومن دون تحمل الخسائر والمخاطر التي يتحملها القائم بالهجوم في إطار استخدامه للأسلحة الحركية التقليدية، وقد توصلت هذي الدول في العقد الأخير إلى أحدث هذي الوسائل التي تتسم بالتعقيد واجتياز الحدود التقليدية، وهي الهجمات السيبرانية التي تؤدي للاحتلال الرقمي للدولة ومنظوماتها، والتي من شأنها التدمير الكلي للبنية التحتية للخصم، والتسبب بأثار فادحة على الاعيان العسكرية والمدنية للخصم، وذلك كله من دون الحاجة إلى الدخول في أي اشتباك حقيقي ومادي مع الطرف الأخر، ومن دون الحاجة لتحمل أعباء مالية ومخاطر المواجهة المسلحة التي يتحملها المهاجم في إطار استخدام الأسلحة التقليدية. ونحن اليوم نرى كميات هائلة من المناوشات المتعلقة بتقنية المعلومات بين روسيا وأوكرانيا تجري عبر الشبكة العالمية، حيث تتجاوز كل دولة على السيادة الدولة الأخرى، حاولت روسيا القضاء على العديد من العناصر الأساسية للبنية التحتية الرقمية في أوكرانيا، بما في ذلك البنوك وشبكات الكهرباء وغيرها من الخدمات عبر الشبكة العالمية أو المتصلة بها، على الرغم من أن أوكرانيا تمكنت إلى حد كبير من صد الهجمات الرقمية، في الوقت نفسه، كانت أوكرانيا تدافع بقوة عن أراضيها في الفضاء الرقمي بالإضافة إلى صد الهجمات الروسية، كانت أوكرانيا أكثر استعدادًا لأي محاولات في مهاجمة روسيا، مما أدى إلى تعطيل بنيتها التحتية الرقمية، خاصة مع التركيز على طرق النقل والتسليم التي سيتم استخدامها لتزويد ودعم القوات المشاركة في النشاط على الأرض.

مشكلة البحث .

إن المشاكل الرئيسة التي تطرح بشأن دراسة الاحتلال الرقمي يثور بعدة تساؤلات، ويمكن تلخيص في عدة تساؤلات رئيسة ومهمة:

- ما الاحتلال الرقمي؟
- هل يمكن نسبة تصرفات المشارك المباشر في الهجمات الرقمية إلى الدول؟
- ما هي التزامات الدول الأساسية بشأن مكافحة اللجوء إلى الهجمات الرقمية وكيف تقوم الدول بالحد من الآثار الضارة لهذه الهجمات، رقميًا وتشريعيًا؟

أهمية الدراسة .

إن لموضوع الاحتلال الرقمي أهمية كبيرة في التوجه القانوني الحديث ويكمن ذلك في عدة أسباب، السبب الأول: ضرورة التصدي جنائيًا وتقنيًا لهذي المشكلات العالمية، والسبب الثاني، الذي يكمن في أهمية اختيار هذه الدراسة هو ازدياد اللجوء إلى الهجمات الرقمية وتزايد مشاركة المدنيين بصورة مباشرة وغير مباشرة في العمليات العسكرية الرقمية، فضلًا عن نشأة الشركات الأمنية والعسكرية والتقنية الخاصة التي تقوم بتقديم دعمها ومنتوجاتها الخاصة بالحروب الرقمية.

منهجية الدراسة .

سنقوم في البحث اعتماد المنهج التحليلي والمقارن بالنظر للأبعاد التي يحملها موضوع البحث، ففي بادئ الأمر سنلجأ للمنهج التحليلي، ومن ثم المقارن في سبيل التوقف على نظرة الفقه الحديثة من هذي الجريمة.

خطة البحث.

المبحث الأول: ماهية الاحتلال الرقمي

المطلب الأول: مفهوم الاحتلال في ظل الذكاء الاصطناعي

المطلب الثاني: خصائص الاحتلال الرقمي

المبحث الثاني: التصدي التشريعي والتقني للاحتلال الرقمي

المطلب الأول: دور التشريعات الوطنية والدولية للاحتلال الرقمي

المطلب الثاني دور التقنيات الذكية في منع جرائم الاحتلال الرقمي

المبحث الأول/ماهية الاحتلال الرقمي.

من نافلة القول بان العصور تتقدم وتطورت، ومع هذا التقدم العلمي في المجال الرقمي ظهرت بواقعنا مُشكلة مُهمة ألا وهي الحروب والهجمات والاحتلال الرقمي، ومنْ مُنطلق أن القانون هو صمام أمان الشعوب صار لِزامًا على التشريعاتِ أن تَبتكر قَواعد قانونية تُساهم في الحَدِّ من هذه الجريمة، كما من الضروري ان تتوفر المصدات التِقنية التي تحافظ على ديمومة المؤسسات في الدولة.

المطلب الأول/مفهوم الاحتلال في ظل الذكاء الاصطناعي.

ان للتطورات التقنية الحديثة الدور الواضح وخاصة تقنيات الذكاء الاصطناعي في ان يكون لهذي التطبيقات في تعزيز التطور العالمي وإنجاز الخدمات والمهام بصورة سريعة، ومع هذا التطور تنامت ظواهر إجرامية في العيد من القطاعات وخاصة القطاعات التي لا توفر المستلزمات اللازمة في التصدي لاي خطر يحدق بها، وكما من المشكلات العملية التي بات واضحة هو استخدام تقنيات الذكاء الاصطناعي في ارتكاب هذي الجرائم الخطرة.ان العالم اليوم يشهد تحديًا كبيرًا وخطرًا وخاصة في مجال التسليح، حيث بات التسليح اليوم بعيدًا عن السلاح، فقد اتجهت نحو التسليح الرقمي، حيث تشكل هذي الخطوات تحديدًا كبيرًا للدول، حيث يقوم هذا التسليح على تطوير وتعزيز القدرات الرقمية في الدولة، من ناحية البنى التحتية الرقمية والتشريعية والبشرية، وهذا بالتأكيد سيخل بتوازن القوى عالميًا، فما نشاهده اليوم من تطورات كبيرة تجعل دولًا عديدة في مرمى نيران الهجمات والحروب الرقمية؛ ويعود السبب في ذلك لافتقار العديد من الدول للمعرفة الرقمية التي تتيح لها التصدي لاي هجمة أو حرب رقمية مستقبلية.

بدأت رحلة الذكاء الاصطناعي لأول مرة بصورة خيال علمي، آلات تتحرك وتفكر وتتحدث، وأول من صك هذا المفهوم -الذكاء الاصطناعي- هو العالم الأمريكي جون مكارثي في العام ١٩٥٦ في مؤتمر دارتموث. إن تقنيات الذكاء الاصطناعي عرفت من قبل أكسفورد بانها نظريات وتطور أنظمة الحاسوب القادرة على أداء المهام التي تقتضي عادةً ذكاء بشري مثل الادراك البصري والتعرف على الكلام، وصنع القرار، والترجمة بين اللغات [1]. تمكن اليوم التقنيات الذكية والتعلم الآلي عبر نظم الذكاء الاصطناعي القدرة العالية للجهات الاجرامية من شن هجمات رقمية ضخمة مصممة لإحداث تأثير على العمليات المجتمعية دون استخدام موارد كبيرة أو مهارات متطورة أو أعداد كبيرة من المنفذين، وتسمح الأمية الرقمية لمستخدمي وسائل التواصل الاجتماعي بعمليات أكثر تطورًا ذات تأثير عالٍ، في ظل الكم المتزايد من انتاج ملفات تعريف مزيفة وصور واصوات وافلام فيديو، وسيتطلب تهديد الهجمات الرقمية المدعومة من الذكاء الاصطناعي الاستثمار في الدفاع الرقمي المعزز بالتقنيات الذكية، علمًا ان الامن الرقمي للتقنيات الجديدة المدعومة بالذكاء الاصطناعي تمثل اليوم تحديًا كبيرًا للمجتمعات كافة ومصدر قلق لها [2]. يعرف الاحتلال الرقمي على انه هجوم يتم عبر الشبكة العالمية يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول اليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات رقمية تقوم بها دولة ضد دولة أخرى [3].كما إن الاحتلال الرقمي تصرف يدور في عالم رقمي قائم على استخدام بيانات رقمية ووسائل اتصال تعمل بصورة رقمية، ومن بعد ذلك شهد تطورًا ليتضمن مفهومًا واسعًا يقوم على تحقيق أهداف عسكرية أو أمنية حساسة ومباشرة، جراء اختراق مواقع إلكترونية حساسة، عادة ما تؤدي وظيفة ذات أولوية في الدولة، كأنظمة حماية المحطات النووية أو الكهربائية أو المطارات ووسائل النقل الأخرى [4]. كما تجدر الملاحظة ان عمليات القصف الرقمي هي صورة من صور الاحتلال الرقمي للمنظومة الرقمية للدولة حيث يعرف بانه أسلوب للهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الرقمية إلى مواقع هذي الشبكات مما يزيد الضغط على قدرتها على استقبال رسائل المتعاملين معها والذي يؤدي إلى وقف عمل الشركة، وعادة ما تلجأ المنظمات الإرهابية لتدمير البنى التحتية الخاصة بأنظمة المعلومات في العالم بأسره [5]. ويجد الباحث من خلال ذلك بأن يعرف الاحتلال الرقمي على انه هجوم رقمي يستهدف البنى التحتية الحرجة للدولة، والسيطرة عليها مما يجعل الحكومة وافرادها غير قادرين على الدخول للمواقع الرسمية ولا التحكم بها،

وتكون تحت سيطرة صاحب الهجوم دولة كانت أو منظمة.ان ما يجب ان ننبه عنه هو سبيل تحديد الدولة المحتلة رقميًا يكون من اللازم ان ننتبه إلى انه يجب ان يصدر التصرف من الدولة المعتدية شخصيًا، وهنا يثور تساؤل مهم في مدى معرفة مصدر الحرب أو الهجوم في ظل استخدام الدول العديد من المراكز أو الجهات الخارجية في الاستهداف؟

تكمن الإجابة في ذلك من خلال تحديد مصدر الهجوم الرقمي وهو بالتأكيد تثور معه عدة مشكلات خاصة في ان التطور الكبير في التقنية يتيح للشخص المهاجم تغير مكانه رقميًا ويكون في مكان ليس هو مصدر الهجوم، حيث يتميز هذا الشرط بانه أكثر تعقيدًا وصعوبة، وهذا الخصيصة يجب ان تكون لمواجهتها مصدات تقنية عالية الدقة في تحديد مصدر الهجوم الحقيقي، لإنه من المتوقع ان يترك الشخص خلفه ثغرة تتيح للدولة معرفة مصدر الهجوم، وهذا التحقيق الرقمي يكون من خلال تقنيات الذكاء الاصطناعي، التي يكون لها القدرة والامكانية في تحديد زمان ومكان المعتدي بدقة عالية. كما من المتوقع ان تقوم جهات خاصة، وغير تابعة للدولة متكونة من أفراد على دول وتقوم باحتلالها رقميًا، كيف سيتم التعامل معها؟

ان معايير ذلك هو انها ستكون عبارة عن مواجهة جنائية وتقنية لهذي الجماعات وعدها هجمات خطرة تستهدف الدولة وبنيتها التحية، ولا يمكن نسبتها للدولة التي وقع في اقليمها مصدر الهجوم طالما انها لم يكن لها أي تدخل فيه، أو أي مساهمة، او دعم، أو حتى الموافقة بعد وقوع الهجوم أو تأيده.

المطلب الثاني/خصائص الاحتلال الرقمي.

ان من الخصائص التي يتصف بها الاحتلال الرقمي هو تعطيل البنى التحتية الحرجة للدولة[6] حيث أكد رئيس وكالة الامن السيبراني الألماني في عام ٢٠٢١ آرني شوينبوم "إن المستشفيات بالبلاد قد تكون تحت خطر متزايد من هجوم رقمي، بعد هجومين تعرضت لهما الخدمات الصحية الأيرلندية وخط انابيب وقود امريكي، وتم استهداف العيادات الألمانية بسلسلة من الهجمات الرقمية على مدى السنوات الخمس الماضية [7]. في البدء، إن **الحروب الرقمية تتم في بيئة رقمية افتراضية**، حيث إن ما يميز هذي الفعل الجرمي عن الجريمة التقليدية في أن الحاسوب والشبكة العالَمية الأداة الرئيسة في ارتكابها، ومحلها هي المعلومات المخزنة على الحاسوب وشبكاته، كما أنها قد ترتكب أثناء إحدى مراحل تشغيل نظام المعالجة الآلية للمعلومات سواء في مرحلة الإدخال أو المعالجة أو الإخراج [8].ومن جانب آخر **الحروب الرقمية متعددة النطاق الجغرافي**، إن التطور التِقني في إطار الحاسبات وبرامجها وشبكات الاتصال وخاصة الشبكة العالَمية جعل النتاج الذهني يتصف بالعالمية، لأنه لا يقتصر على دولة دون أخرى، فالبشرية شريكة في الاستفادة من هذا الإنتاج الأدبي والفني إلى جانب ذلك فإن الاستخدام غير المشروع لهذه الوسيلة والشبكة اتصف أيضًا بالعالمية أو بالعابرة للحدود فالجرائم لم تعد مقتصرة على إقليمٍ محدد ولا أيضًا تتعداه، بل أصبح بالإمكان ارتكاب جرائم عبر الحاسوب بالولوج إليه واختراقه من بلد آخر أو إتلافه، ومن الأمثلة على هذا هو تمكن الهواة في أوربا في حل شفرة أحد مراكز المعلومات في البنتاجون (وزارة الدفاع الأمريكية) ومن ثَم أصبح المجال أمامه مفتوح للعبث ببيانات المركز وهو الحال في إنتاج الفيروسات [9].ومن منطلق التطبيقات العملية التي تتصدى لهذا النوع من الجرائم أن نذكر ما جاء في المادة ٢٦ من قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها "تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه حتى ولو ارتكبت كُلِيًا أو جُزْئِيًا خارج إقليم الدول، متى أضرت بأحد مصالحها ويختص القضاء الوطني بنظر الدعاوى المترتبة عليها" [10]. وفي ذات السياق نجد هنالك من المناسب ذكر خاصية أخرى يتصف بها الاحتلال الرقمي وهي أن **الاحتلال الرقمي بطبيعته صعب ان تثبت جهة التنفيذ**، حيث يوصف الاثبات في هذا النوع من العمليات من أبرز التحديات التي تواجه الأجهزة الأمنية، ويزداد الإثبات صعوبة في الاحتلال الرقمي، حيث إن اكتشاف هذي الجريمة أمر ليس بالسهل، ولكن حتى في حال اكتشاف وقوع الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به الكثير من الصعوبات، لأن هذه الجريمة تتم في بيئة غير تقليدية حيث إنها تقع خارج

إطار الواقع المادي الملموس، وبالإضافة إلى ذلك فإن نقص الخبرة الفنية والتِقنية لدى الجهات المختصة يشكل عائقًا أَسَاسِيًا أمام إثبات الفعل الرقمي، ذلك أن هذا النوع من الجرائم يتطلب تدريب وتأهيل هذي الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة الحاسوب والشبكة العالَمية ونتيجة لنقص الخبرة والتدريب كثيرًا ما تخفق الأجهزه في تقدير أهمية الجريمة هذي، فلا تبذل لكشف غموضها وضبط مرتكبها جهودًا تناسب وهذي الأهمية، بل إن المحقق قد يدمر الدليل بمحوه عن خطأ منه أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة [11].

المبحث الثاني/ التصدي التشريعي والتقني للاحتلال الرقمي.

إن ظهور الحاسوب والشبكة العالمية "الإنترنت" من أبرز تطورات العلم الحديث في هذا العصر، وخطوة جلية للبشرية، حيث تقدمت بالإنجازات وخدمة جلية للإنسانية في مناحي حياة عديدة، منها الاقتصادية، والتعليمية، والقانونية، والطبية، والكثير من المجالات الأخرى، ورافق هذي التصورات ظهور خبراء يمتلكون القدرة والقابلية على تطويع هذي التقنيات لصالحهم واستغلالها في سبيل ارتكاب العديد من الجرائم، فما كان على الدول الا ان تتصدى لذلك من خلال ادواتها التشريعية وكذلك الاستعانة بالخبرات التقنية وخاصة تقنيات الذكاء الاصطناعي للحد من هذي الظواهر التي تؤثر على المجتمع واستقراره.

المطلب الأول/ دور التشريعات الدولية والوطنية للاحتلال الرقمي.

كانت منظمة الأمم المتحدة دائمة السعي لتأمين سلامة استخدام التقنية والشبكات المعلوماتية بصورة عامة، وتشارك كلا من الجمعية العامة ومجلس الأمن ومكتب مكافحة الإرهاب التابع للأمم المتحدة في مختلف المفاوضات لتوافق الآراء من أجل وضع معايير توفر الحماية للشبكة العالمية [12] وسوف نبين ذلك فيما يلي:

الجمعية العامة:

- القرارين 63/55 و121/56 اللذين يضعان الإطار القانوني بشأن "مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية".
- القرار 57/239 المتعلق بـ "إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي".
- القرار 58/199 المتعلق بـ إرساء ثقافة عالمية الأمن الفضاء الحاسوبي وحماية الهياكل الأساسية الحيوية للمعلومات.
- القرار 73/187 المتعلق بـ "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الجرمية".
- القرار ٧٤/١٧٣ المتعلق بـ "تعزيز المساعدة التقنية وبناء القدرات لتدعيم التدابير الوطنية والتعاون الدولي في مجال مكافحة الجريمة السيبرانية، بما يسمح تبادل المعلومات".

ويبدو أن الأمم المتحدة مستعدة للقيام بدور ريادي، فقد أعربت الدول الأعضاء للأمم المتحدة، في الاستعراض السادس للاستراتيجية العالمية لمكافحة الإرهاب في القرار ٢٨٤/٧٢ الصادر عن الجمعية العامة، عن قلقها إزاء تزايد استخدام الإرهابيين تكنولوجيا المعلومات والاتصالات، وخاصة الشبكة العالمية وغيرها من الوسائط لارتكاب الأعمال الإرهابية أو التحريض عليها أو التجنيد لها وتمويلها أو التخطيط لها.

مجلس الأمن:

- القرار ٢٣٤١ (٢٠١٧)، الذي يهيب فيه الدول الأعضاء إلى إنشاء أو تعزيز الشراكات الوطنية والإقليمية والدولية مع الجهات صاحبة المصلحة من القطاعين العام والخاص، حسب الاقتضاء، التبادل المعلومات والخبرات من أجل منع الهجمات الإرهابية على الهياكل الأساسية الحيوية والحماية منها

والتخفيف من آثارها والتحقيق فيها ومواجهتها والتعافي من أضرارها، وذلك بوسائل منها التدريب المشترك واستخدام أو إنشاء شبكات ملائمة للاتصال والإنذار في حالات الطوارئ، وأيضا يسلم بأن جهود الحماية تتوزع على مسارات متعددة منها أمن الفضاء الرقمي".

– القرار ٢٣٧٠ (٢٠١٧)، الذي يحث فيه الدول الأعضاء على العمل بصورة تعاونية لمنع الإرهابيين من حيازة الأسلحة، من خلال تكنولوجيات المعلومات والاتصالات، مع احترام حقوق الإنسان والحريات الأساسية والامتثال للالتزامات بموجب القانون الدولي".

بعد التطورات التي رافقت العالم الرقمي بادر الاتحاد الأوروبي في صياغة العديد من الاستراتيجيات في معالجة هذي المخاطر، وفي تحديث صادر في الشهر الخامس من العام ٢٠٢٢، حيث وافقت الدول الأعضاء في الاتحاد الأوروبي على تنفيذ تدابير أكثر صرامة للأمن الرقمي عبر الاتحاد، وتشرف الإستراتيجية المنقحة على الكيانات المتوسطة والكبيرة التي تنتمي إلى "القطاعات الحيوية"، بما في ذلك مزودي خدمات الاتصالات الرقمية العامة، والخدمات الرقمية، وإدارة مياه الصرف الصحي والنفايات، وتصنيع المنتجات المهمة، والخدمات البريدية والبريدية، والإدارة العامة، على الصعيدين المركزي وعلى المستوى الإقليمي، وقطاع الصحة [13]. إن السعي الحثيث للاتحاد الأوروبي في مجال الامن السيبراني يبين مدى أهمية ان تعير الدول الأهمية القصوى لهذا الموضوع لما يشكله من خطورة فائقة، حيث تمكن التقنيات الرقمية من احتلال الدول رقميًا بسهولة في حالة عدم وجود مصدات تشريعية وتقنية مناسبة لصد هذا الخطر، فالاحتلال الرقمي الذي يكون من خلال استهداف البنى التحتية للدولة هو مصدر قلق دولي، فكما اتاحت هذي التقنيات الحرب عن بُعد من غير استخدام طرق تقليدية في الهجوم، فيمكن ان تحتل هذي الدول أي دولة تريد رقميًا. كما إن الصعيد العربي لم يكن بعيدًا عن التطورات التي ترافق العالم التقني وما صاحبة من مشكلات، حيث بذلت الجهود الكبيرة في مكافحة الجرائم السيبرانية، وأسفر ذلك بوضع اتفاقية عربية لمكافحة جرائم تقنية المعلومات، والتي انبثقت عن الاجتماع المشترك لمجلس وزراء الداخلية والعدل العرب، الذي عقد بمقر الأمانة العامة لجامعة الدول العربية في عام (2010م)؛ وكان الهدف من هذي الاتفاقية تعزيز التعاون بين الدول العربية في مكافحة جرائم تقنية المعلومات، والجرائم السيبرانية التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، وتلبية الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وقد جاءت هذه الاتفاقية من منطلق الالتزام بالمعاهدات والمواثيق العربية والدولية المتعلقة بهذا الشأن [14].كما ان الدول سعت من خلال تشريعاتها الوطنية في رفد منظومتها الأمنية للتصدي للهجمات الرقمية؛ بما تشكله من تهديد حقيقي للدولة، ومما يؤسف له القول في ان العراق ولغاية الآن لم يتبنى أي تشريع خاص لمكافحة مثل هكذا جرائم والتصدي لها، وهذا ما يجعل التصدي تشريعيًا في محل إشكاليات عديدة.ونذكر من الدول العربية التي تصدت عبر استراتيجياتها الوطنية في التصدي لاحتلال الرقمي، ومنها:

– الجمهورية العربية مصر: مهدت الخطة القومية للاتصالات وتقنية المعلومات الطريق للبدء في مبادرة مجتمع المعلومات المصري الذي يضع الأسس لتطوير مجتمع المعلومات المصري حتى عام 2020 ففي 2003 جددت مصر خطتها القومية للاتصالات والمعلومات من خلال مبادرة مجتمع المعلومات المصرية، وتم تفصيل استراتيجية ورؤية مجتمع المعلومات المصري وثيقة بناء جسور رقمية، رؤية مصر في مجتمع المعلومات، والتي قدمت في المرحلة الأولى من WSIS واستعرضت هذي الوثيقة تقدم مصر في تحقيق مجتمع معلوماتها، وتضمنت هذي الرؤية سبعة محاور أساسية وهي:

1 - تحضير رقمي يتعامل مع تطور وتجديد شبكة الاتصالات في مجال الهواتف الثابتة والمحمولة.

2 - حكومة إلكترونية تستهدف توفير الخدمات إلى المواطنين والمستثمرين في مواقعهم بسرعة وسهولة من خلال الشبكة العالمية.

3 - اعمال إلكترونية تستهدف تحويل المجتمع المصري إلى مجتمع معلومات يتماشى مع التنمية الدولية ويصل إلى تكنولوجيا العصر.
4 - تعليم الكتروني يستهدف نشر المعرفة والمعلومات التي تستخدم وسائل تكنولوجية الكترونية.
5 - تطوير خدمات صحية تستخدم تقنية المعلومات لرفع كفاءة تقديم خدمات علاجية وطبية عن بعد خاصة في المناطق البعيدة.
6 - توثيق إلكتروني للتقاليد الطبيعية والحضارية عن طريق بناء أنظمة معلومات متكاملة للتقديم المحلي والعالمي للحضارة المصرية.
7 - تطوير الصناعات التقنية من خلال رفع مستوى النوعية للشركات المصرية ورفع قدراتها العالمية على المنافسة.

وبهذا نجد ان من المرافق المهمة والحيوية في الدولة ومدى خطورة استهدافها واحتلالها من قبل الدول أو الجماعات الاجرامية، لذا يكون من اللازم ان تعير الدولة أهمية قصوى في تأمينها وإدخال التِقنية الحديثة في كل مفاصلها الحيوية، من خلال تِقنيات الذكاء الاصطناعي والأدوات التشريعية في الدولة.

إضافة لذلك شرع في مصر قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الذي يعد القانون الأول في معالجة مثل هكذا جرائم، ويعد القوة الضاربة تشريعيًا في سبيل كل شخص يستهدف البنى التحتية الحرجة للدولة مستهدفًا أيها من أجل احتلال الدولة رقميًا.وتجدر الإشارة إلى ان العراق وفي العام ٢٠٢٢ اقر الاستراتيجية الوطنية للأمن السيبراني، وهي تُعد خطوة استباقية لمواجهة المخاطر الرقمية وحماية البنى التحتية للدولة رقميًا، حيث ستمكن هذي الخطوة من ضمان وحماية الوجود العراقي في الفضاء الرقمي، وبناء منظومة شبكية موثوق بها، حيث ان الوجود العالمي وخاصة المجال الاقتصاد يعتمد على ما تحققه الدولة من قوة رقمية، حيث ستوفر هذي الاستراتيجية الامن للبنى التحتية الحيوية للمعلومات وغيرها من العناصر الحرجة في نظام المعلومات في ظل الوقت الراهن، فالمخاطر الرقمية هي احتمال وجود تهديد وهشاشة داخل الفضاء الرقمي للبلد يضر بأمن وسلامة نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية.

المطلب الثاني/ دور التقنيات الذكية في منع جرائم الاحتلال الرقمي.

يمثل الذكاء الاصطناعي الصورة الواضحة في التصدي للهجوم وخاصة الهجمات الرقمية التي تمس البنى التحتية الحرجة، فالعالم الحديث تتحول فيه الحروب من حروب واقعية إلى حروب رقمية ووصولًا لاحتلال الدولة رقميًا، وكما نعلم ان غالبية الدول حولت التعامل إلى التعامل الالكتروني أو هي في طور التطور والسعي في التحول للنحو الرقمنة في الخدمات، وما يشكله الذكاء الاصطناعي اليوم من قوة عسكرية دفاعية لا بُدَّ منها كما من الازم ان تسعى الدول في سبيل انشاء منظومة عسكرية عالية المستوى في التصدي للهجمات الرقمية. كانت الحرب الرقمية عنصرًا رئيسيًا في المعركة الدائرة بين روسيا وأوكرانيا وهي متداخلة بصورة فريدة تقريبًا مع مساحة الحرب المادية والحركية في هذا الصراع، بدلاً من رؤية الحرب الرقمية والجسدية كمساحتين منفصلتين، سعى كلا الجانبين لإقناع مصلحتهما وزيادة الهجمات الجسدية بهجمات رقمية معاصرة، يُنظر إلى هذا بصورة أفضل في مثال يوم واحد في وقت مبكر من الصراع عندما شن قراصنة روس هجومًا على مذيع إعلامي أوكراني مهم - تمامًا كما أعلن الجيش الروسي عن نيته تدمير أهداف "التضليل" الأوكرانية وتوجيه ضربة صاروخية ضد جهاز تلفزيون، إنه مؤشر على مدى تكامل الحرب الرقمية للجيش الحديث ولماذا نحتاج إلى أن نكون على دراية بما هو قادم. وفي خضم هذا الصراع التقني في الاستفادة من تقنيات الذكاء الاصطناعي، فان الاستراتيجيات العسكرية في الدفاع الرقمي تعرف بانها مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثير الهجمات الإلكترونية، والتخفيف من حدتها والتعافي منها بسرعة، والتجربة النمساوية في استراتيجيتها عدت مصطلح الدفاع الرقمي بانه جميع التدابير اللازمة للدفاع عن الفضاء الرقمي بالوسائل المناسبة لتحقيق الأهداف العسكرية الاستراتيجية، وبخصوص الاستراتيجية العسكرية

البلجيكية عدت الدفاع الرقمي بانه تطبيق التدابير الوقائية الفعالة للحصول على مستوى مناسب من الأمن الرقمي، وتقليل المخاطر الأمنية إلى مستوى مقبول، وفيما يتعلق بالتجربة الفرنسية مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع عن نظم المعلومات الحرجة في الفضاء الرقمي [15].فالبنى التحية المعلوماتية الحرجة تمثل نقطة استهداف من قبل الدول والجماعات المسلحة الرقمية في المستقبل مستغلين تقنية الذكاء الاصطناعي في تحقيق أهدافهم الخبيثة، وهذا يعين ان على الدول التجهيز لمواجهة هذا النوع من الهجمات في المستقبل من خلال تطوير أنظمة دفاع رقمية تتصدى لهذا النوع من الهجمات وبصورة مبكرة، وهذا يتحقق من خلال برامج ذكاء اصطناعي متكامل له القدرة على كشف المخاطر مسبقًا. ان المقصود بالاستراتيجية منع الجريمة هو منهج أو إطار قائم في منع الجريمة وحصر معدلات ارتكابها وهذا يتم من خلال العديد من الوسائل المتنوعة والكفيلة بتحقيق ذلك، وتعتمد الاستراتيجية في خطتها لمنع الجريمة على عدة مقومات أساسية وتعد بمنزلة ركائز أو دعائم يتعين توافرها ويمكن حصرها في القيم الفكرية وسلامة التوجه، وكفاءة الأجهزة المنفذة، وفعالية القوانين العقابية [16]. وفي مجال أحدث الاستراتيجيات الوطنية للأمن السيبراني، كشفت إيطاليا عن استراتيجيتها الوطنية للأمن السيبراني، والوثيقة تستعرض ثلاث تهديدات إلكترونية رئيسية ومجالات عمل، ومن بينها النشاط الإجرامي أي الهجمات الإلكترونية التي أطلقها مجرمو الإنترنت أو نشطاء القرصنة أو حملات الدولة المنسقة التي تستغل أخطاء البرامج والتكوين الخاطئ ونقاط الضعف في البروتوكولات أو البشر لسرقة البيانات أو تدمير الأنظمة، بالإضافة لذلك، هناك المرونة الرقمية للإدارة العامة أي التكنولوجيا التي تستخدمها الدولة وملحقاتها [17].كما ان استخدام الذكاء الاصطناعي في الأمن الرقمي، حيث يمكن استخدام تقنيات الذكاء الاصطناعي لمعرفة كيفية إزالة الضوضاء أو البيانات غير المرغوب فيها وتمكين خبراء الأمن من فهم البيئة الرقمية من أجل اكتشاف النشاط غير الطبيعي، حيث يمكن الذكاء الاصطناعي من توليد تقنيات مؤتمتة حين يشعر بتهديد أمني رقمي، فالذكاء الاصطناعي يملك القدرة على تحليل عدد كبير من البيانات والسماح بتطوير الأنظمة والبرامج الحالية بطريقة مناسبة للحد من الهجمات الرقمية [18].

تشكل الجرائم التي ترتكب في البيئة الرقمية اليوم صور من صور التهديدات العالمية الواسعة، مهددة بذلك اقتصاديات الدول ومنظوماتها، حيث نجد الدول تسعى بصورة حثيثة من اجل تطوير منظوماتها الأمنية الرقمية كحدود رقمية جديدة مثلها مثل الحدود الجغرافية الطبيعية، مشيدة لذلك جدارًا رقميًا يحافظ على أنظمتها الرقمية من أي تهديد أو تجاوز تتعرض له، فالدول تروم لتطوير ذلك من خلال الحفاظ على الحدود الرقمية كما تحافظ على حدودها الطبيعية، فالحدود الرقمية تمثل أهمية عالية يجب حمايتها بصورة آمنة وعالية المستوى، فلا يمكن ان نواجه خطر التهديدات الأمنية من دون وجود بُنية تشريعية عالية المستوى، وكذلك وجود بُنية تحتية معلوماتية تساعد الجهات المختصة في رفد المنظومة الأمنية بفريق عمل ومعدات تواجه هذا الخطر، وخير هذي الأدوات هي أدوات وتقنيات الذكاء الاصطناعي [19].

وفي ضوء الاستعدادات التي تبديها الدول في سبيل الحفاظ على منظوماتها الرقمية أنشأت مؤسسات خاصة من أجل ذلك، حيث أعلنت وكالة مشاريع الأبحاث الدفاعية المتقدمة التابعة لوزارة الدفاع الأميركية "داربا (DARPA) "عن إطلاق برنامج جديد يُسمى "ضمان متانة الذكاء الاصطناعي ضد الخداع(GARD) "، وأوضحت الوكالة أنه صمم لتطوير دفاعات جديدة ضد الهجمات العدائية الموجهة ضد نماذج التعلم الآلي، كما ويهدف البرنامج إلى الرد على أنظمة الذكاء الاصطناعي العدائية من خلال تطوير اختبارات لتحديد خصائص دفاعات التعلم الآلي المختلفة وتقييم قابليتها للتطبيق، وقدم الباحثون العاملون في البرنامج موارد وطوروا أدوات افتراضية ومواد تدريبية ومجموعة بيانات معيارية، متاحة للجميع، لتسهيل التبادل المفتوح للأفكار والأدوات والتقنيات التي يمكن أن تساعد الباحثين في اختبار وتقييم دفاعات نماذج التعلم الآلي الدفاعية الحالية والناشئة [20].وكما بينا بان الهجمات الرقمية تشكل تهديدًا عالميًا مستمرًا وأصبحت أكثر تعقيدًا وصعوبة، يمكن أن تؤدي انتهاكات الأمن الرقمي إلى دخول

المتسللين إلى الحسابات المصرفية وحسابات وسائل التواصل الاجتماعي والمزيد وتسريب البيانات الخاصة وسرقة تقنية المعلومات المتطورة الخاصة بأسلحة الدمار الشامل وتعطيل البنى التحتية للدول.

حيث ما تزال الدول تبذل الجهد الكبير في تعزيز الأمن الرقمي بعد سلسلة الهجمات الرقمية التي طالت العديد من الدول، وباتت ذات مخاطر ومسببة في أضرار بالغة في القطاعات والمؤسسات والبنى التحتية، وتتعالى الأصوات الدولية بتأسيس تحالف دولي ضد الهجمات الرقمية واستحدثت القوى العظمى داخل صفوف جيوشها الوطنية وحدات رقمية جديدة للتصدي للهجمات الرقمية بما في ذلك الهجمات باستخدام برمجية الفدية.

الخاتمة.

في الختام وبعد هذا العرض، تبين لنا ما للهجمات الرقمية من ضرر وخطر يشكله هذا الفعل المعدي بالنهاية لاحتلا الدولة رقميًا، وهذا الضرر يصيب كل افراد المجتمع من خلال استخدام المجرم أساليب غير تقليدية، كما ان قوة هذي الجريمة في التأثير على البناء المؤسساتي الرقمي للدولة، حيث إن هذي الجريمة تكون أكثر صعوبة لما تتصف بها من خصوصية، ولهذا سيورد الباحث أهم النتائج التي توصل إليها خلال البحث، وأيضًا السعي في ذكر مجموعة من التوصيات التي تُكَوِّن إجابة لتساؤل الدراسة الرئيس.

النتائج:

1 – يعرف الاحتلال الرقمي على انه هجوم رقمي يستهدف البنى التحتية الحرجة للدولة، والسيطرة عليها مما يجعل الحكومة وافرادها غير قادرين على ان الدخول للمواقع الرسمية ولا التحكم بها.

2 – تشكل الجرائم المعلوماتية اليوم صور من صور التهديدات العالمية الواسعة، مهددات بذلك اقتصاديات الدول ومنظوماتها.

3 – يمثل الذكاء الاصطناعي الصورة الواضحة في التصدي للهجوم وخاصة الهجمات الإلكترونية التي تمس البنى التحتية الحرجة، فالعالم الحديث تتحول فيه الحروب من حروب واقعية إلى حروب إلكترونية.

التوصيات:

1 - ضرورة الاهتمام بتحديث استراتيجيات الأمن السيبراني بصورة دورية، وكذلك الاستعانة بالخبرات التقنية والفنية في سبيل تعزيز منظومة الدولة رقميًا.

2 - الاستعانة بتقنيات الذكاء الاصطناعي وتعلم الآلة في مجال التنبؤ بالهجمات الرقمية، والتصدي لها بصورة استباقية، قبل الوصول للاحتلال الرقمي للدولة المُعتدية.

3 - ضرورة تبني قوانين تقنية واتفاقيات دولية في مجال التصدي للعمليات الرقمية التي تستهدف البنى التحتية الحرجة للدولة، وهذا من خلال مبادرة الأمم المتحدة باتفاقية عالمية جديدة.

4 - عدّ الهجمات الرقمية التي تكون من دولة على دولة أخرى واحتلالها رقميًا بانها جرائم دولية تضاف للنظام الأساس الخاص بالمحكمة الدولية الجنائية، وينعقد اختصاص النظر فيها للمحكمة المختصة في الدولة بالجرائم الدولية أو المحكمة الدولية الجنائية.

الهوامش.

---

(1) د. لينا أحمد الفراني، سماهر أحمد حامد القرني، الذكاء الاصطناعي القائم على التعليم الآلي المايكروبيت Micro: bit لتنمية مهارات البرمجة وقياس دافعية طالبات الصف الأول الثانوي، المجلة الدولية للعلوم التربوية والنفسية، مجلد ٢٠، العدد ٣٩، المؤسسة العربية للبحث العلمي والتنمية البشرية، السعودية، ٢٠٢٠، ص ١١.

(2) د. ممدوح عبد الحميد عبد المطلب، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، دار النهضة العربية، مصر، القاهرة، ٢٠٢٠، ص ٩.

(3) د. احمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي

المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد ٨، العدد ٤، كلية القانون، جامعة بابل، ٢٠١٦، ص ٦١٦.

(4) زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير، كلية القانون، جامعة الكوفة، العراق، ٢٠١٦، ص ١٣.

(5) عمر عباس خضير العبيدي، مكافحة الجرائم السيبرانية كآلية لتعزيز الأمن الإقليمي، مركز الدراسات العربية، مصر، القاهرة، 2021، ص 37.

(6) عرفت البنية التحتية المعلوماتية الحرجة في مصر بانها "مجموعة من أنظمة أو شبكات أو اصول معلوماتية أساسية يؤدي الكشف عن تفصيلاتها تعطيلها أو تغيير طريقة عملها بطريقة غير مشروعة، أو الدخول غير المصرح به عليها، أو الدخول أو الوصول بشكل غير قانوني للبيانات والمعلومات التي تحفظها أو تعالجها، أو يؤدي القيام بأي فعل غير مشروع آخر بها إلى التأثير على توافر خدمات الدولة ومرافقها الاساسية أو خسائر اقتصادية أو اجتماعية كبيرة على المستوى الوطني، ويعد من البنية التحتية المعلوماتية الحرجة على الاخص ما =يستخدم في الطاقة الكهربائية الغاز الطبيعي والبترول، الاتصالات، والجهات المالية والبنوك، والصناعات المختلفة، والنقل والموصلات والطيران المدني، والتعليم والبحث العلمي، والبث الاذاعي والتليفزيوني، ومحطات مياة الشرب والصرف الصحي والموارد المائية، والصحة، والخدمات الحكومية وخدمات الإغاثة وخدمات الطوارئ، وغيرها من مرافق المعلومات والاتصالات التي تقد تؤثر على الأمن القومي أو الاقتصاد القومي والمصلحة العامة وما في حكمها". قرار رئيس مجلس الوزراء المصري رقم ١٦٩٩ لسنة ٢٠٢٠ بإصدار اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.

(7) حازم سعيد، الهجمات والحروب السيبرانية: خطوات استباقية للحروب التقليدية، يمكن الوصول له عبر الرابط: https://www.politics-dz.com، تاريخ النشر ٢٠٢١/٨/١٩، تاريخ الزيارة ٢٠٢٢/٥/١٤.

(8) حسين عباس حميد، نحو اختصاص محكمة إلكترونية خاصة بالجرائم المعلوماتية، رسالة ماجستير، جامعة الاسكندرية، كلية الحقوق، مصر، ٢٠٢٠، ص ٢٢.

(9) أ. سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانون، العدد ١٠، جامعة محمد خيضر- بسكرة، ٢٠١٠، ص٢٨١.

(10) اعتمد من قبل جامعة الدول العربية الأمانة الفنية لمجلس وزراء العدل العرب مشروع القانون العربي الاسترشادي لمكافحة جرائم المعلوماتية" بالصيغة المرفقة، بعد تعديل تسميته ليصبح "قانون الامارات العرب الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها"، والطلب إلى الأمانة العامة =تعميمه على وزارات الداخلية في الدول العربية الأعضاء، للاستفادة منه بقرار ٤١٧، د ٢٠٠٤/٢١م.

(11) حسين عباس حميد، مرجع سابق، ص ٢٣.

12 د. جورج لبكي، المعاهدات الدولية للإنترنت: حقائق وتحديات، مجلة الدفاع الوطني، بيروت، العدد ٨٣، كانون الثاني ٢٠١٣.

(13) European commission – press release.

(14) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

(15) د. عائشة عبد الحميد، الإطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي، المجلة الدولية للذكاء الاصطناعي في التعليم والتدريب، المجلد ١، العدد ١، جمعية التنمية التكنولوجية والبشرية، ٢٠٢١، ص ١٤.

(16) د. سعد عاطف عبد المطلب حسنين، دور الشرطة في مكافحة الجرائم السيبرانية المستحدثة وتحقق الامن المعلوماتي دراسة مقارنة، مجلة بحوث كلية، العدد ٣٠، جامعة المنوفية، كلية الآداب، مصر، ٢٠١٩، ص ٤٨٨.

(17) Strategia Nazionale Di Cybersicurezza 2022- 2026.

(18) عادل عبد الله حميد وفدوة سعد البواردي، مكافحة الفساد -تحديات الذكاء الاصطناعي والأمن السيبراني-، المتحدة للطباعة والنشر، الامارات، أبو ظبي، ٢٠٢١، ص ٥٨.

(19) حسين المولى، الهندسة الاجتماعية والذكاء الاصطناعي، صحيفة الصباح، العدد ٥٢٨٤، شبكة الإعلام العراقي، العراق، بغداد، ٢٠٢١، ص ١١.

(20) Lamar Johnson, Darpa Launches program to Build AI Resiliency Against Adversaries, accessible at: www.meritalk.com, last visited 19/5/2022, visit data 4/1/2022.

المصادر.
الاتفاقيات:
-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
-قانون الامارات العرب الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها"، والطلب إلى الأمانة العامة تعميمه على وزارات الداخلية في الدول العربية الأعضاء، للاستفادة منه بقرار ٤١٧، د ٢٠٠٤/٢١م.
القوانين:
-قرار رئيس مجلس الوزراء المصري رقم ١٦٩٩ لسنة ٢٠٢٠ بإصدار اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.
الكتب:
-عادل عبد الله حميد وفدوة سعد البواردي، مكافحة الفساد -تحديات الذكاء الاصطناعي والأمن السيبراني، المتحدة للطباعة والنشر، الامارات، أبو ظبي، ٢٠٢١.
-عمر عباس خضير العبيدي، مكافحة الجرائم السيبرانية كآلية لتعزيز الأمن الإقليمي، مركز الدراسات العربية، مصر، القاهرة، 2021.
-ممدوح عبد الحميد عبد المطلب، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، دار النهضة العربية، مصر، القاهرة، ٢٠٢٠.
الرسائل:
-حسين عباس حميد، نحو اختصاص محكمة إلكترونية خاصة بالجرائم المعلوماتية، رسالة ماجستير، جامعة الاسكندرية، كلية الحقوق، مصر، ٢٠٢٠.
-زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير، كلية القانون، جامعة الكوفة، العراق، ٢٠١٦.
الابحاث:
-احمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد ٨، العدد ٤، كلية القانون، جامعة بابل، ٢٠١٦.
-جورج لبكي، لبكي، المعاهدات الدولية للإنترنت: حقائق وتحديات، مجلة الدفاع الوطني، بيروت، العدد ٨٣، كانون الثاني ٢٠١٣.
-سعد عاطف عبد المطلب حسنين، دور الشرطة في مكافحة الجرائم السيبرانية المستحدثة وتحقق الامن المعلوماتي دراسة مقارنة، مجلة بحوث كلية، العدد ٣٠، جامعة المنوفية، كلية الآداب، مصر، ٢٠١٩.
-سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانون، العدد ١٠، جامعة محمد خيضر- بسكرة، ٢٠١٠.
-عائشة عبد الحميد، الإطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي، المجلة الدولية للذكاء الاصطناعي في التعليم والتدريب، المجلد ١، العدد ١، جمعية التنمية التكنولوجية والبشرية، ٢٠٢١.
-لينا أحمد الفراني، سماهر أحمد حامد القرني، الذكاء الاصطناعي القائم على التعليم الآلي المايكروبيت Micro: bit لتنمية مهارات البرمجة وقياس دافعية طالبات الصف الأول الثانوي، المجلة الدولية للعلوم التربوية والنفسية، مجلد ٢٠، العدد ٣٩، المؤسسة العربية للبحث العلمي والتنمية البشرية، السعودية، ٢٠٢٠.
المقالات:
-حسين المولى،الهندسة الاجتماعيةوالذكاء الاصطناعي،صحيفة الصباح، العدد ٥٢٨٤،شبكة الإعلام العراقي،العراق، بغداد، ٢٠٢١.
المواقع الإلكترونية:
-حازم سعيد، الهجمات والحروب السيبرانية: خطوات استباقية للحروب التقليدية، يمكن الوصول له عبر الرابط: https://www.politics-dz.com، تاريخ النشر ٢٠٢١/٨/١٩، تاريخ الزيارة ٢٠٢٢/٥/١٤.
المصادر الأجنبية:
- European commission – press release.
- Lamar Johnson, Darpa Launches program to Build AI Resiliency Against Adversaries, accessible at: www.meritalk.com, last visited 19/5/2022, visit data 4/1/2022.
- .2026 -Strategia Nazionale Di Cybersicurezza 2022